

10/534541

JC20 Rec'd PCT/PTO 10 MAY 2005

#2

DOCKET NO.: 271813US90PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yukio TSURUOKA, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/JP04/09944

INTERNATIONAL FILING DATE: July 12, 2004

FOR: AUTHENTICATION SYSTEM BASED ON ADDRESS, DEVICE THEREOF, AND PROGRAM

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION**

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<u>COUNTRY</u>	<u>APPLICATION NO</u>	<u>DAY/MONTH/YEAR</u>
Japan	2003-273445	11 July 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP04/09944. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Surinder Sachar

Masayasu Mori
Attorney of Record
Registration No. 47,301
Surinder Sachar
Registration No. 34,423

Customer Number

22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

Rec'd PCT/PTO 10 MAY 2005

PCT/JP2004/009944

10/534541

14.7.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application: 2003年 7月 11日

出願番号
Application Number: 特願 2003-273445

[ST. 10/C]: [JP 2003-273445]

出願人
Applicant(s): 日本電信電話株式会社

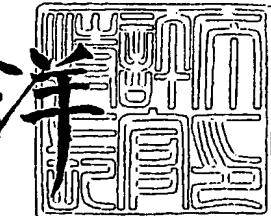
REC'D 02 SEP 2004
WIPO PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 8月 19日

特許庁長官
Commissioner,
Japan Patent Office

八 月 洋



【書類名】 特許願
【整理番号】 NTTT155555
【提出日】 平成15年 7月11日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 17/60
【発明者】
 【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
 【氏名】 鶴岡 行雄
【発明者】
 【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
 【氏名】 菊地 能直
【発明者】
 【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
 【氏名】 水野 伸太郎
【発明者】
 【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
 【氏名】 高橋 健司
【発明者】
 【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
 【氏名】 唐澤 圭
【特許出願人】
 【識別番号】 000004226
 【氏名又は名称】 日本電信電話株式会社
【代理人】
 【識別番号】 100066153
 【弁理士】
 【氏名又は名称】 草野 卓
【選任した代理人】
 【識別番号】 100100642
 【弁理士】
 【氏名又は名称】 稲垣 稔
【手数料の表示】
 【予納台帳番号】 002897
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9806848

【書類名】特許請求の範囲**【請求項1】**

ユーザを認証する認証サーバと、ユーザを認証するためのユーザ認証情報を送信するユーザ端末と、ユーザの認証後にユーザ端末を介してユーザにサービスを提供するアプリケーションサーバとがネットワークを介して通信可能に接続された認証システムにおいて、認証サーバは、

ユーザ端末から送信されたユーザ認証情報に基づいてユーザ認証データを蓄積するユーザデータベースを参照してユーザの認証を行う認証手段と、

ユーザの認証が成功したとき、ユーザ端末にアドレスを割当てるアドレス割当手段と、

アドレス割当手段によって割当てられたアドレスを含むチケットを発行するチケット発行手段と、

チケット発行手段によって発行されたチケットをユーザ端末に送信するチケット送信手段を備え、

ユーザ端末は、

認証サーバから送信されたチケットを受信するチケット受信手段と、

チケットに含まれるアドレスを送信元アドレスに設定する手段と、

チケットを含むパケットをアプリケーションサーバに送信する手段と、

送信元アドレスを含むサービスの要求を表すパケットをアプリケーションサーバに送信するサービス要求手段を備え、

アプリケーションサーバは、

ユーザ端末から送信されたチケットを記憶するチケット記憶手段と、

チケット記憶手段が記憶したチケットに含まれるアドレスとユーザ端末から送信されたサービスの要求を表すパケットに含まれる送信元アドレスとが一致するか否かを判断するアドレス判断手段と、

アドレス判断手段によってアドレスが一致すると判断されたときユーザにサービスを提供するサービス提供手段を備えたことを特徴とするアドレスに基づく認証システム。

【請求項2】

ユーザを認証する認証サーバと、ユーザを認証するためのユーザ認証情報及びユーザ側の公開鍵に関する鍵情報を送信するユーザ端末と、ユーザの認証後にユーザ端末を介してユーザにサービスを提供するアプリケーションサーバとがネットワークを介して通信可能に接続された認証システムにおいて、

認証サーバは、

ユーザ端末から送信されたユーザ認証情報に基づいてユーザ認証データを蓄積するユーザデータベースを参照してユーザの認証を行う認証手段と、

ユーザの認証が成功したとき、ユーザ端末から送信された鍵情報を対応させるアドレスを割当てるアドレス割当手段と、

アドレス割当手段によって割当てられたアドレス及び鍵情報を含むチケットを発行するチケット発行手段と、

チケット発行手段によって発行されたチケットをユーザ端末に送信するチケット送信手段とを備え、

ユーザ端末は、

鍵情報と関連する鍵ペアとアプリケーションサーバの公開鍵からアプリケーションサーバと共有するセッション秘密鍵を計算する手段と、

チケットに含まれるアドレスを送信元アドレスに設定する手段と、

チケットを含むパケットをアプリケーションサーバに送信する手段と、

送信元アドレスを含むサービスの要求を表すパケットをアプリケーションサーバに送信するサービス要求手段を備え、

アプリケーションサーバは、

鍵情報と関連するユーザ側の公開鍵とアプリケーションサーバの鍵ペアからユーザ端末と共有するセッション秘密鍵を計算する手段と、

ユーザ端末から送信されたチケットを記憶するチケット記憶手段と、鍵情報とセッション秘密鍵の計算に用いられたユーザ側の公開鍵が対応するか否かを検証する手段と、

鍵情報とユーザ側の公開鍵が対応すると検証されたとき、チケット記憶手段に記憶したチケットに含まれるアドレスとサービスの要求を表すパケットに含まれる送信元アドレスとが一致するか否かを判断するアドレス判断手段と、

アドレス判断手段によってアドレスが一致すると判断されたときユーザにサービスを提供するサービス提供手段を備えたことを特徴とするアドレスに基づく認証システム。

【請求項3】

アプリケーションサーバは、

ユーザ端末から送信されたチケットを検証するチケット検証手段を備え、

チケット記憶手段は、チケット検証手段によってチケットが正しいことが検証されたときチケットを記憶し、それ以外のときチケットを記憶しないことを特徴とする請求項1または2に記載のアドレスに基づく認証システム。

【請求項4】

認証サーバのチケット発行手段は、

認証サーバとアプリケーションサーバとの間で事前に共有する共有秘密鍵を用いて仮のチケットから認証子を一時的に生成し、生成された認証子を含むチケットを発行し、

アプリケーションサーバのチケット検証手段は、

チケットに含まれる認証子及び認証サーバとアプリケーションサーバとの間で事前に共有する共有秘密鍵を用いてチケットを検証し、

アプリケーションサーバのチケット記憶手段は、

チケットが正しいことが検証されたときチケットを記憶し、それ以外のときチケットを記憶しないことを特徴とする請求項3に記載のアドレスに基づく認証システム。

【請求項5】

認証サーバのチケット発行手段は、

チケットの有効期限を表す情報およびタイムスタンプを含むチケットを発行し、

アプリケーションサーバのチケット検証手段は、

チケットに含まれるタイムスタンプおよび有効期限を表す情報に基づいてチケットが有効期限内であることを検証し、

アプリケーションサーバのチケット記憶手段は、

チケットが有効期限内であることが検証されたときチケットを記憶し、それ以外のときチケットを記憶しないことを特徴とする請求項3または請求項4に記載のアドレスに基づく認証システム。

【請求項6】

ユーザ端末は、

アプリケーションサーバとの間でセッション秘密鍵を共有し、セッション秘密鍵を用いてパケットの情報から計算された認証ヘッダを、パケットに付加し、

アプリケーションサーバのチケット検証手段は、

受信したパケットに付加された認証ヘッダをユーザ端末とのセッションで共有されるセッション秘密鍵を用いて検証することを特徴とする請求項1乃至5の何れか1項に記載のアドレスに基づく認証システム。

【請求項7】

認証サーバは、

ユーザの認証が成功したとき、ユーザと対応するユーザ識別子を割当てるユーザ識別子割当手段を備え、

チケット発行手段は、

ユーザ識別子を含むチケットを発行することを特徴とする請求項1乃至6の何れか1項に記載のアドレスに基づく認証システム。

【書類名】明細書

【発明の名称】アドレスに基づく認証システム

【技術分野】

【0001】

本発明は、ユーザ端末がユーザの認証を認証サーバに要求し、認証サーバが認証の要求に応じてユーザを認証する認証システムに関する。より詳細には、ユーザの認証後に認証サーバが、認証の要求に応じてチケットを発行し、発行したチケットに基づいてアプリケーションサーバがユーザ端末を介してユーザにサービスを提供する認証システムに関する。

【背景技術】

【0002】

従来のネットワーク認証システムにおいては、ユーザが接続サービスを利用する時に、接続認証サーバが、顧客情報とユーザIDとの対応関係が予め格納されている個人情報データベースを参照してそのユーザを認証し、その認証が成功した場合に、接続の許可と共にIP(Internet Protocol)アドレスをユーザの端末に割当て、割当てたIPアドレスをユーザ端末に送信すると同時にIPアドレスとユーザIDの関係を記憶装置に保持し、商取引サービス利用時にユーザ端末が、接続認証サーバから送信されたIPアドレスを用いてインターネット上の販売サービス提供装置に購入する商品を申込み、販売サービス提供装置は、この商品の購入申込からIPアドレスを取得し、取得したIPアドレスを元に記憶装置からユーザIDを取得し、その取得したユーザIDと対応する顧客情報を取得することにより、顧客の認証を行うものが知られている（例えば、特許文献1参照。）。

【特許文献1】特開2002-207929 (請求項1および図2)

【発明の開示】

【発明が解決しようとする課題】

【0003】

しかしながら、上述の従来の認証システムは、ユーザの接続認証時やサービス提供時に、第三者が、ユーザが使用しているIPアドレスをネットワーク上に送受されるパケットから盗み出し、盗み出したアドレスを用いて商取引サービスを提供するサーバにアクセスすることにより、第三者によって成りすましが可能となってしまう課題が残されていた。換言すれば、従来の認証システムでは、ユーザに割当てたアドレスの正当性を保証することができない。なお、正当なアドレスとは、ISP(internet service provider)などの機関がユーザまたはユーザの端末に対して正当な手順に従って割当てたアドレスである。

本発明は、このような従来の課題を解決するためになされたもので、ユーザに割当てたアドレスの正当性を保証することができるアドレスに基づく認証システムを提供するものである。

【課題を解決するための手段】

【0004】

請求項1に記載のアドレスに基づく認証システムは、ユーザを認証する認証サーバと、ユーザを認証するためのユーザ認証情報を送信するユーザ端末と、ユーザの認証後にユーザ端末を介してユーザにサービスを提供するアプリケーションサーバとがネットワークを介して通信可能に接続された認証システムにおいて、認証サーバは、

ユーザ端末から送信されたユーザ認証情報に基づいてユーザ認証データを蓄積するユーザデータベースを参照して前記ユーザの認証を行う認証手段と、ユーザの認証が成功したとき、ユーザ端末にアドレスを割当てるアドレス割当手段と、アドレス割当手段によって割当てられたアドレスを含むチケットを発行するチケット発行手段と、チケット発行手段によって発行されたチケットをユーザ端末に送信するチケット送信手段を備え、

ユーザ端末は、

認証サーバから送信されたチケットを受信するチケット受信手段と、チケットに含まれるアドレスを送信元アドレスに設定する手段と、チケットを含むパケットをアプリケーション

ヨンサーバに送信する手段と、送信元アドレスを含むサービスの要求を表すパケットをアプリケーションサーバに送信するサービス要求手段を備え、

アプリケーションサーバは、

ユーザ端末から送信されたチケットを記憶するチケット記憶手段と、チケット記憶手段が記憶したチケットに含まれるアドレスとユーザ端末から送信されたサービスの要求を表すパケットに含まれる送信元アドレスとが一致するか否かを判断するアドレス判断手段と、アドレス判断手段によってアドレスが一致すると判断されたときユーザにサービスを提供するサービス提供手段を備えたことを特徴とする。

この構成により、認証サーバがユーザに割当てたアドレスを含むチケットを発行し、ユーザ端末が、発行されたチケットをアプリケーションサーバに送信し、アプリケーションサーバが、送信されたチケットを記憶し、記憶したチケットに含まれるアドレスに基づいてユーザ端末から送信されたパケットを、認証されたユーザのパケットとみなすことにより、アドレスに基づく認証が可能となる。

【0005】

請求項2に記載のアドレスに基づく認証システムは、

ユーザを認証する認証サーバと、ユーザを認証するためのユーザ認証情報及びユーザ側の公開鍵に関する鍵情報を送信するユーザ端末と、ユーザの認証後にユーザ端末を介してユーザにサービスを提供するアプリケーションサーバとがネットワークを介して通信可能に接続された認証システムにおいて、

認証サーバは、

ユーザ端末から送信されたユーザ認証情報に基づいてユーザ認証データを蓄積するユーザデータベースを参照してユーザの認証を行う認証手段と、ユーザの認証が成功したとき、ユーザ端末から送信された鍵情報と対応させるアドレスを割当てるアドレス割当手段と、アドレス割当手段によって割当てられたアドレス及び鍵情報を含むチケットを発行するチケット発行手段と、チケット発行手段によって発行されたチケットをユーザ端末に送信するチケット送信手段を備え、

ユーザ端末は、

鍵情報と関連する鍵ペアとアプリケーションサーバの公開鍵からセッション秘密鍵を計算する手段と、チケットに含まれるアドレスを送信元アドレスに設定する手段と、チケットを含むパケットをアプリケーションサーバに送信する手段と、

送信元アドレスを含むサービスの要求を表すパケットをアプリケーションサーバに送信するサービス要求手段を備え、

アプリケーションサーバは、

鍵情報と関連するユーザ側の公開鍵とアプリケーションサーバの鍵ペアからセッション秘密鍵を計算する手段と、ユーザ端末から送信されたチケットを記憶するチケット記憶手段と、チケットに含まれる鍵情報とセッション秘密鍵の計算に用いられたユーザ側の公開鍵が対応するか否かを検証する手段と、鍵情報とユーザ側の公開鍵が対応すると検証されたとき、記憶したチケットに含まれるアドレスとサービスの要求を表すパケットに含まれる送信元アドレスとが一致するか否かを判断するアドレス判断手段と、アドレス判断手段によってアドレスが一致すると判断されたときユーザにサービスを提供するサービス提供手段とを備えたことを特徴とする。

この構成により、認証サーバが、ユーザまたはユーザ端末と対応した鍵情報を対応させるアドレスを含むチケットを発行し、ユーザ端末が、発行されたチケットをアプリケーションサーバに送信し、アプリケーションサーバが、送信されたチケットを記憶し、記憶したチケットに含まれるアドレスに基づいてユーザ端末から送信されたパケットを、認証されたユーザのパケットとみなすことにより、アドレスに基づく認証が可能となる。

【0006】

請求項3に記載のアドレスに基づく認証システムは、

請求項1または2に記載のアドレスに基づく認証システムにおいて、

アプリケーションサーバは、

ユーザ端末から送信されたチケットを検証するチケット検証手段を備え、チケット記憶手段は、チケット検証手段によってチケットが正しいことが検証されたときチケットを記憶し、それ以外（unknown）のときチケットを記憶しないことを特徴とする。

この構成により、チケットが正しいことを検証したときチケットを記憶するため、アプリケーションサーバが検証したチケットに含まれるアドレスに基づいてユーザ端末から送信されたパケットを、認証されたユーザのパケットとみなすことにより、アドレスに基づく認証が可能となる。

【0007】

請求項4に記載のアドレスに基づく認証システムは、

請求項3に記載のアドレスに基づく認証システムにおいて、

認証サーバのチケット発行手段は、

認証サーバとアプリケーションサーバとの間で事前に共有する共有秘密鍵を用いて仮のチケットから認証子を一時的に生成し、生成された認証子を含むチケットを発行し、

アプリケーションサーバのチケット記憶手段は、

チケット検証手段によってチケットに含まれる認証子および共有秘密鍵を用いてチケットが正しいことが検証されたときチケットを記憶し、それ以外のときチケットを記憶しないことを特徴とする。

この構成により、アプリケーションサーバが認証サーバとの間で事前に共有する共有秘密鍵を用いて生成される認証子からチケットを検証するため、認証サーバによって発行されたチケットの正当性を保証することができる。

【0008】

請求項5に記載のアドレスに基づく認証システムは、

請求項3または請求項4に記載のアドレスに基づく認証システムにおいて、

認証サーバのチケット発行手段は、

チケットの有効期限を表す情報およびタイムスタンプを含むチケットを発行し、

アプリケーションサーバのチケット記憶手段は、

チケット検証手段によってチケットに含まれるタイムスタンプおよび有効期限を表す情報に基づいて前記チケットが有効期限内であることが検証されたときチケットを記憶し、それ以外のときチケットを記憶しないことを特徴とする。

この構成により、認証サーバがチケットの有効期限を表す情報を含むチケットを発行し、アプリケーションサーバがサービスの有効期限を検証するため、認証サーバの運営方針に従って有効期限を決定することができる。

【0009】

請求項6に記載のアドレスに基づく認証システムは、

請求項1乃至5の何れか1項に記載のアドレスに基づく認証システムにおいて、

ユーザ端末のサービス要求手段は、

アプリケーションサーバとのセッションで共有されるセッション秘密鍵を計算し、計算されたセッション秘密鍵を用いて得られた認証ヘッダを、パケットに付加してアプリケーションサーバに送信し、

アプリケーションサーバのチケット検証手段は、受信された前記パケットに付加された認証ヘッダをセッション秘密鍵を用いて検証することを特徴とする。

この構成により、チケットが正しいことを検証したときチケットを記憶させるため、認証サーバによって発行されたチケットの正当性を保証することができ、また、ユーザ端末がアプリケーションサーバとのセッションで共有されるセッション秘密鍵を計算し、計算されたセッション秘密鍵を用いて得られた認証ヘッダをアプリケーションサーバが検証するため、ユーザ端末とアプリケーションサーバとの間で送受されるパケットのインテグリティをより高めることができる。

【0010】

請求項7に記載のアドレスに基づく認証システムは、

請求項1乃至6のいずれか1項に記載のアドレスに基づく認証システムにおいて、認証サーバは、

ユーザの認証が成功したとき、ユーザと対応するユーザ識別子を割当てるユーザ識別子割当手段を備え、

チケット発行手段は、ユーザ識別子を含むチケットを発行することを特徴とする。

この構成により、チケットに含まれるユーザ識別子に基づきサービスの提供に伴う課金などを行うことができる。

【発明の効果】

【0011】

以上説明したように、本発明は、ユーザに割当てたアドレスの正当性を保証することができるアドレスに基づく認証システムを提供するものである。

【発明を実施するための最良の形態】

【0012】

以下、図面を参照して本発明の実施の形態について詳細に説明する。

(第1の実施の形態) アドレスに基づく認証システム

図1は、本発明の第1の実施の形態に係るアドレスに基づく認証システムのシステム構成図である。図1に示すように、アドレスに基づく認証システム1000は、ユーザを認証する認証サーバ100と、ユーザを認証するためのユーザ認証情報を送信する複数のユーザ端末200を収容するアクセスポイント30と、ユーザの認証後にユーザ端末200を介してユーザにサービスを提供する複数のアプリケーションサーバ300とが、ネットワーク10を介して通信可能に接続された構成を有している。

なお、認証サーバ100には、ユーザに関する情報(ユーザ認証データ)が格納されているユーザデータベース20が接続されている。ユーザは、ユーザ端末200を利用する利用者に限定されず、計算機上のデータを含むオブジェクトであってもよい。また、アドレスに基づく認証システム1000は、ユーザ端末200とアプリケーションサーバ300とに接続される回線の安全性が物理的に確保される構成でもよい。

また、ネットワーク10は、無線、有線を問わず、LAN(Local Area Network)またはインターネットなどによって構成されてもよい。アクセスポイント30は、地域毎に設置されてもよい。ユーザ端末200は、無線の通信が可能な携帯端末、若しくは、パソコンなどの端末でもよい。また、アプリケーションサーバ300は、映画およびスポーツ番組を含むコンテンツ配信サービス、電子商取引などのサービス、電子メール、IP電話、およびインスタントメッセージなどの通信サービス、またはWorld Wide Webなどの情報閲覧サービスを提供するサーバである。

【0013】

ユーザ端末200は、ユーザを認証するためのユーザ認証情報をアクセスポイント30を介して認証サーバ100に送信することによりユーザの認証を要求するようになっている。本実施例においては、ユーザ認証情報には、ユーザ名およびパスワード、ユーザを認証するための鍵ペアに基づいて生成された情報、またはユーザの生体(例えば、指紋、虹彩、静脈パターン、筆跡、声紋等)を認証するための情報のうち少なくとも1つが含まれる。なお、鍵ペアは、公開鍵暗号技術に基づいた公開鍵と秘密鍵のペアである。

認証サーバ100は、ユーザ端末200から送信されたユーザ認証情報に基づいてユーザデータベース20を参照してユーザの認証を行い、ユーザの認証が成功したとき、ユーザと対応するユーザ識別子を割当て、割当てたユーザ識別子と対応させるユーザ端末を一意に特定可能なアドレスを割当て、割当てたアドレスおよびユーザ識別子を含むチケットを発行し、発行されたチケットをユーザ端末200に送信するようになっている。

ユーザ端末200は、認証サーバ100から送信されたチケットに含まれるアドレスを送信元アドレスに設定してアプリケーションサーバ300にチケットを送信すると共にサービスを要求するようになっている。

アプリケーションサーバ300は、ユーザ端末200によって送信されたチケットを記憶し、記憶したチケットに含まれるアドレスとサービスの要求を表すパケットに含まれる

送信元アドレスとが一致するか否かを判断し、アドレスが一致すると判断されたときユーザーにサービスを提供するようになっている。

【0014】

(第1の実施の形態) 認証サーバ

図2は、本発明の第1の実施の形態に係る認証サーバのブロック構成図である。図2に示すように、認証サーバ100は、通信インターフェース101および制御処理手段102を含むように構成される。また、通信インターフェース101は、例えば、モデムまたはLANインターフェースなどによって構成され、ネットワーク10と接続される通信装置と通信可能にするものであれば如何なるものによって構成されてもよい。

制御処理手段102は、プログラムを処理するCPU(Central Processing Unit)、およびプログラムを記憶するメモリなどを含むように構成される。また、制御処理手段102は、ユーザ認証情報受信手段110、認証手段120、ユーザ識別子割当手段130、アドレス割当手段140、チケット発行手段150、およびチケット送信手段160を有している。なお、これらの手段はプログラムのモジュールでもよい。

なお、認証サーバ100には、ユーザに関する情報が格納されているユーザデータベース20が接続されており、ユーザデータベース20は、ユーザを認証するときに使用する認証データ、およびユーザIDを含むユーザID登録データを有している。

【0015】

ユーザ認証情報受信手段110は、ユーザ端末200から送信されたユーザ認証情報などを通信インターフェース101を介して受信するようになっている。

認証手段120は、ユーザ認証情報受信手段110によって受信されたユーザ認証情報に基づいてユーザの認証を行うようになっている。例えば、認証手段120は、ユーザ認証情報とユーザデータベース20に格納されている認証データとの整合性を検証することによってユーザを認証するようになっている。

ユーザ識別子割当手段130は、ユーザの認証が成功したとき、ユーザと対応するユーザ識別子を割当てるようになっている。ここで、ユーザ識別子は、ユーザ端末に割当てたアドレスに基づく認証システム1000において一意の識別子である。

あるいはユーザ識別子は、認証サーバ内で一意な識別子をA、認証サーバのグローバルIPアドレスをBとしたとき、「A@B」などのように、グローバルに一意性を満たすよう拡張可能なものであってもよい。

例えば、ユーザ識別子割当手段130は、ユーザデータベース20に格納されているユーザID登録データからユーザIDを取得し、取得したユーザIDをユーザ識別子として割当るようになっている。なお、ユーザ識別子割当手段130は、ユーザIDを取得したときに乱数を生成し、生成した乱数を取得したユーザIDに付加した情報をさらに認証サーバ100の秘密鍵で暗号化したものをユーザ識別子として割当てるようにもよい。この場合には、秘密鍵を知る者、例えば認証サーバ100のみがユーザ識別子に基づいてユーザIDを知ることができるために、ユーザのプライバシー保護を実現できる。また、ユーザ識別子割当手段130は、ユーザ認証情報からユーザ識別子を割当るようにもよい。

アドレス割当手段140は、ユーザ識別子割当手段130によって割当てたユーザ識別子と対応させるアドレスをユーザ端末に割当てるようになっている。なお、アドレスは、IPアドレスの他、メールアドレス、SIP(Session Initiation Protocol)で扱われるURI(Uniform Resource Identifier)、またはIM(Instant Messaging)の相手名でもよい。

チケット発行手段150は、認証子生成手段151を含むように構成され、ユーザ識別子割当手段130によって割当てられたユーザ識別子とアドレス割当手段140によって割当てられたアドレスとを含む仮のチケットを一時的に生成し、認証子生成手段151によって生成される認証子を含めたチケットを発行する。

【0016】

なお、チケットは、アドレスおよびユーザ識別子の他に、チケットを発行したときのタ

イムスタンプ、チケットの有効期限を表す情報、ユーザ端末200に割当てられた帯域幅を表す情報、およびユーザ端末200が収容されるアクセスポイント30に関する情報、例えば位置情報等などによって構成されるようにしてもよい。

なお、チケットの有効期限を表す情報、およびユーザ端末200に割当てられた帯域幅を表す情報は、アクセスポイント30、認証サーバ100およびアプリケーションサーバ300などを運用する通信事業者やアプリケーションサービス事業者と、ユーザ端末200を使用するユーザとの契約によって予め決められるようにしてもよい。

認証子生成手段151は、アプリケーションサーバ300との間で事前に共有する共有秘密鍵と一方向性ハッシュ関数とを用いて、チケット発行手段150が一時的に生成した仮のチケットから認証子を生成するようになっている。なお、認証子生成手段151は、認証子に代えて認証サーバ100の秘密鍵を用いてデジタル署名を生成するようにしてもよい。また、チケット発行手段150は、共有秘密鍵を用いてチケット51全体を暗号化するようにしてもよい。チケット51全体を暗号化するときには、アプリケーションサーバ300が正常に復号化できたことを確認するためのチェックサムをパケットに含める。

ここで、図5は、チケットの構成及びアプリケーションサーバの処理を示す図である。図5に示すように、チケット51は、割当てられたアドレス、ユーザ識別子、および認証子などによって構成される。

チケット送信手段160は、チケット発行手段150によって発行されたチケット51を通信インターフェース101を介してユーザ端末200に送信するようになっている。

【0017】

(第1の実施の形態) ユーザ端末

図3は、本発明の第1の実施の形態に係るユーザ端末のブロック構成図である。図3に示すように、ユーザ端末200は、通信インターフェース201および制御処理手段202を含むように構成される。また、通信インターフェース201は、例えば、有線もしくは無線のLANインターフェース、モ뎀、または携帯電話などの通信機器などによって構成され、アクセスポイント30を介してネットワーク10と接続される通信装置と通信可能にするものであれば如何なるものによって構成されてもよい。

制御処理手段202は、プログラムを処理するCPU、およびプログラムを記憶するメモリなどを含むように構成される。また、制御処理手段202は、認証要求手段203およびサービス要求手段230を有している。なお、これらの手段はプログラムのモジュールでもよい。また、認証要求手段203は、ユーザ認証情報生成手段210、ユーザ認証情報送信手段220、およびチケット受信手段231を有している。

ユーザ認証情報生成手段210は、ユーザ名およびパスワードを表す情報などを含むユーザ認証情報を生成するようになっている。例えば、ユーザ認証情報生成手段210は、キーボードなどの入力機器40からユーザ名およびパスワードを入力させ、入力された情報に応じてユーザ認証情報を生成するようになっている。なお、ユーザ名およびパスワードの他、ユーザ認証情報には、ユーザを認証するための鍵ペアに基づいて生成された情報、またはユーザの生体を認証するための情報のうち少なくとも1つが含まれていてもよい。

【0018】

ユーザ認証情報送信手段220は、ユーザ認証情報生成手段210によって生成されたユーザ認証情報を通信インターフェース201を介して認証サーバ100に送信するようになっている。

サービス要求手段230は、セッション確立手段232を含むように構成され、アプリケーションサーバ300が提供するサービスを要求するようになっている。

チケット受信手段231は、認証サーバ100から送信されたチケット51を通信インターフェース201を介して受信し、受信したチケット51に含まれるアドレスを通信インターフェース201に登録するようになっている。なお、サービス要求手段230が、受信したチケット51に含まれるアドレスを送信元アドレスとして通信インターフェース201に登録するようにしてもよい。

【0019】

セッション確立手段232は、ユーザが利用するサービスに応じたアプリケーションサーバ300とのセッションを確立するようになっている。例えば、セッション確立手段232は、送信元アドレス及びチケット受信手段231によって受信されたチケット51を通信インターフェース201を介してアプリケーションサーバ300に送信することにより、セッションを確立するようになっている。

ここで、図6は、チケット送信時のパケットの構成及びアプリケーションサーバの処理を示す図である。図6に示すように、パケット52は、送信元アドレスおよびチケット51などによって構成される。

例えば、セッション確立手段232は、パケット52を通信インターフェース201を介してアプリケーションサーバ300に送信するようになっている。なお、通信インターフェース201は、チケット受信手段231によって登録されたアドレスをパケット52に含まれる送信元アドレスに設定し、設定したパケット52を送信するようになっている。サービス要求手段230は、確立したセッションを通してサービスの要求を表すパケットを通信インターフェース201に設定したチケット51のアドレスを用いてアプリケーションサーバ300に送信するようになっている。

【0020】

(第1の実施の形態) アプリケーションサーバ

図4は、本発明の第1の実施の形態に係るアプリケーションサーバのブロック構成図である。図4に示すように、アプリケーションサーバ300は、通信インターフェース301および制御処理手段302を含むように構成される。また、通信インターフェース301は、例えば、モデムまたはLANインターフェースなどによって構成され、ネットワーク10と接続される通信装置と通信可能にするものであれば如何なるものによって構成されてもよい。

制御処理手段302は、プログラムを処理するCPU、およびプログラムを記憶するメモリなどを含むように構成される。また、制御処理手段302は、サービス提供手段310、セッション確立手段311、およびチケット記憶手段330を有している。なお、これらの手段はプログラムのモジュールでもよい。

【0021】

サービス提供手段310は、アドレス判断手段312を含むように構成され、ユーザ端末200から要求されるサービスを提供するようになっている。

セッション確立手段311は、チケット検証手段320を含むように構成され、ユーザ端末200とのセッションを確立するようになっている。なお、セッションを確立する手順の中で、セッション確立手段311は、ユーザ端末200から送信されたチケット51を含むパケット52を受信するようになっている。

チケット検証手段320は、パケット52に含まれるチケット51を検証するようになっている。また、チケット検証手段320は、認証サーバ100との間で事前に共有する共有秘密鍵と、チケット51に含まれる認証子とに基づいてチケット51を検証するようにもよい。また、チケット51全体が暗号化されているときには、チケット検証手段320が共有秘密鍵を用いてチケット51全体を復号化するようになっている。

また、チケット検証手段320は、チケット51に含まれるタイムスタンプおよび有効期限を表す情報に基づいてチケット51が有効期限内か否かによってチケット51を検証するようにもよい。また、サービス提供手段310が、チケット51に含まれるタイムスタンプおよび有効期限を表す情報に基づいてユーザの要求するサービスが有効期限内か否かを検証するようにもよい。

また、チケット検証手段320は、チケット51に含まれるアドレスとパケット52に含まれる送信元アドレスとを照合することによってチケット51を検証するようにしてもよい。

チケット検証手段320がチケット51に含まれるアドレスとパケット52に含まれる送信元アドレスとを照合した結果が一致しており、チケットが正しいアドレスを持つユー

ザ端末から送信されていると判断したとき、チケット記憶手段330は、チケット51を記憶するようになっている。

アドレス判断手段312は、サービスの要求を表すパケットに含まれる送信元アドレスとチケット51に含まれるアドレスとが一致するか否かを検証するようになっている。サービス提供手段310は、チケット51に含まれるアドレスとパケットに含まれる送信元アドレスが一致したとき、ユーザ端末200から要求されるサービスを提供するようになっている。

また、サービス提供手段310は、チケット51に含まれるユーザ識別子に基づき、必要に応じて、ユーザ情報を認証サーバ100に問い合わせてもよい。また、サービス提供に伴う課金などの情報を認証サーバ100を経由してユーザデータベース20に送信してもよい。

【0022】

(第1の実施の形態) アドレスに基づく認証システムの処理

本発明の第1の実施の形態に係るアドレスに基づく認証システムの処理について、図面を参照して説明する。

図7は、本発明の第1の実施の形態に係るアドレスに基づく認証システムの処理を示すシケンス図である。まず、ユーザの認証を要求するとき、ユーザ認証情報が、ユーザ端末200によってアクセスポイント30を介して送信される。ユーザ端末200から送信されたユーザ認証情報に基づいて、ユーザの認証が認証サーバ100によって行われる。ユーザの認証が成功したとき、ユーザ端末に割当てたアドレスおよびユーザ識別子などを含むチケット51が、認証サーバ100によって発行され、ユーザ端末200に送信される。

ユーザ端末200とアプリケーションサーバ300とのセッションの確立を要求するとき、チケット51を含むパケット52は、ユーザ端末200によってアプリケーションサーバ300に送信される。パケット52は、アプリケーションサーバ300によって受信され、チケット51の正当性が検証される。検証したチケットが正しいと検証されたとき、チケット51が記憶される。

次に、アプリケーションサーバ300に対してサービスを要求するとき、サービスの要求を表すパケットは、確立したセッションを通してユーザ端末200によってアプリケーションサーバ300に送信される。記憶したチケット51に含まれるアドレスとサービスの要求を表すパケットに含まれる送信元アドレスとが一致するか否かがアプリケーションサーバ300によって判断され、アドレスが一致すると判断されたときサービスがユーザに提供される。

【0023】

(第1の実施の形態) 認証サーバの処理

図8は、本発明の第1の実施の形態に係る認証サーバの処理の流れを示すフローチャートである。

まず、ユーザ端末200から送信されたユーザ認証情報は、ユーザ認証情報受信手段110によって通信インターフェース101を介して受信され(S101)、ユーザ認証情報に基づいて認証手段120によってユーザの認証が行われ、ユーザの認証が成功したとき、処理はS103へ進み、ユーザの認証が失敗したとき、処理は終了する(S102)。

ユーザの認証が成功したとき、ユーザと対応するユーザ識別子が、ユーザ識別子割当手段130によって割当てられ(S103)、ユーザ識別子割当手段130によって割当てられたユーザ識別子と対応させたアドレスが、アドレス割当手段140によって割当てられる(S104)。

次に、ユーザ識別子割当手段130によって割当てられたユーザ識別子と、アドレス割当手段140によって割当てられたアドレスを含む一時に生成された仮のチケットが、チケット発行手段150によって生成され、認証子生成手段151によって、アプリケーションサーバ300との間で事前に共有する共有秘密鍵と一方向性ハッシュ関数とを用い

て前記仮のチケットに対する認証子が生成される（S105）。

次に、認証子生成手段151によって生成された認証子を含むチケット51が、チケット発行手段150によって発行され（S106）、チケット送信手段160によって通信インターフェース101を介してユーザ端末200に送信される（S107）。

【0024】

（第1の実施の形態）ユーザ端末の処理

図9は、本発明の第1の実施の形態に係るユーザ端末の処理の流れを示すフローチャートである。

まず、ユーザ名およびパスワードを表す情報などを含むユーザ認証情報は、ユーザ認証情報生成手段210によって生成され（S201）、ユーザ認証情報送信手段220によって通信インターフェース201を介して認証サーバ100に送信される（S202）。

認証サーバ100から送信されたチケット51は、チケット受信手段231によって受信される（S203）。チケット51が受信された後、アプリケーションサーバ300とのセッションは、セッション確立手段232によって確立される（S204）。

アプリケーションサーバ300とのセッションが確立された後、サービスの要求を表すパケットは、サービス要求手段230によってセッションを通してアプリケーションサーバ300に送信されることによって、サービスがアプリケーションサーバ300に要求される（S205）。

【0025】

（第1の実施の形態）アプリケーションサーバの処理

図10は、本発明の第1の実施の形態に係るアプリケーションサーバの処理の流れを示すフローチャートである。

まず、ユーザ端末200とのセッションの確立は、セッション確立手段311によって開始され（S301）、パケット52に含まれるチケット51がアプリケーションサーバ300によって受信される。チケット51は、チケット検証手段320によって検証され、チケット51が正しいと検証されたとき、処理はS303へ進み、チケット51が改竄されているなど正しくないと検証されたとき、処理は終了する（S302）。

チケット51が正しいと検証されたとき、セッションは、セッション確立手段311によって確立され、チケット51がチケット記憶手段330に記憶される（S303）。ユーザ端末200から送信されたサービスを要求するパケットに含まれる送信元アドレスと記憶したチケット51に含まれるアドレスとが一致するか否かがアドレス判断手段312により判断され、アドレスが一致すると判断されたとき、サービスが、サービス提供手段310によってユーザ端末200を介してユーザに提供される（S304）。

【0026】

以上説明したように、本発明の第1の実施の形態に係るアドレスに基づく認証システムは、認証サーバ100が、割当てたアドレスおよびユーザ識別子を含むチケット51を発行し、ユーザ端末200が、発行されたチケット51をアプリケーションサーバに送信し、アプリケーションサーバ300が、送信されたチケット51を検証すると共に記憶し、ユーザ端末200から送信されたパケットに含まれる送信元アドレスと記憶したチケット51に含まれるアドレスとを照合することにより、認証されたユーザのパケットとみなすことにより、アドレスに基づく認証が可能となる。

また、アプリケーションサーバ300が認証サーバ100との間で事前に共有する共有秘密鍵を用いて生成される認証子によってチケット51の正当性を検証するため、認証サーバ100によって発行されたチケット51の正当性を保証することができる。

また、認証サーバ100がチケット51の有効期限を表す情報を含むチケット51を発行し、アプリケーションサーバ300が前記有効期限によってチケット51の有効性を検証するため、認証サーバ100の運営方針に従って有効期限を決定することができる。

【0027】

（第2の実施の形態）アドレスに基づく認証システム

図11は、本発明の第2の実施の形態に係るアドレスに基づく認証システムのシステム

構成図である。図11に示すように、アドレスに基づく認証システム2000は、ユーザを認証する認証サーバ400と、ユーザを認証するためのユーザ認証情報を送信する複数のユーザ端末500を収容するアクセスポイント30と、ユーザの認証後にユーザ端末500を介してユーザにサービスを提供する複数のアプリケーションサーバ600とが、ネットワーク10を介して通信可能に接続された構成を有している。

ユーザ端末500は、無線の通信が可能な携帯端末、または、パソコンなどの端末でもよい。また、アプリケーションサーバ600は、映画、スポーツ番組を含むコンテンツ配信サービス、電子商取引などのサービス、電子メール、IP電話、およびインスタントメッセージなどの通信サービス、World Wide Webなどの情報閲覧サービスを提供するサーバである。なお、ユーザは、ユーザ端末500を利用する利用者に限定されず、計算機上のデータを含むオブジェクトであってもよい。

また、ユーザ端末500は、ユーザ端末500に対応した公開鍵暗号化技術に基づいた公開鍵と秘密鍵とが対をなす端末鍵ペアを有してもよく、ユーザに対応した公開鍵と秘密鍵とが対をなすユーザ鍵ペアを認証デバイス41(図13)から入力するようにしてもよい。ここで、端末鍵ペアは、ユーザ端末500に組み込まれているセキュリティチップ等で生成、管理されていてもよい。

【0028】

ユーザ端末500は、ユーザを認証するためのユーザ認証情報をアクセスポイント30を介して認証サーバ400に送信することによりユーザの認証を要求するようになっている。本実施例においては、ユーザ認証情報には、ユーザ名およびパスワード、ユーザを認証するための鍵ペアに基づいて生成された情報、またはユーザの生体を認証するための情報のうち少なくとも1つが含まれる。

また、ユーザ端末500は、鍵情報をユーザ認証情報と共に送信するようになっている。なお、鍵情報は、ユーザ鍵ペアの公開鍵または端末鍵ペアの公開鍵、これらの公開鍵を含む証明書、または公開鍵もしくは公開鍵を含む証明書に一方向性ハッシュ関数を適用して得られたハッシュ値など、公開鍵に関連する情報(ユーザ鍵ペアまたは端末鍵ペアと関連する情報)を含む。この鍵情報に関連する鍵ペアは、ユーザを認証するための鍵ペアと同一でもよい。

また、鍵情報は、事前にユーザ端末500とアプリケーションサーバ600間で共有するアプリケーション認証用共有秘密鍵の所有を証明できる情報であってもよい。例えば、上記アプリケーション認証用共有秘密鍵を入力として計算されたタイムスタンプに対する認証子などである。

認証サーバ400は、ユーザ端末500から送信されたユーザ認証情報に基づいてユーザデータベース20を参照してユーザの認証を行い、ユーザの認証が成功したとき、ユーザと対応するユーザ識別子を割当て、割当てたユーザ識別子と対応させるアドレスを割当て、割当てたアドレス、ユーザ識別子、およびユーザ端末から送信された鍵情報を含むチケットを発行し、発行されたチケットをユーザ端末500に送信するようになっている。

ユーザ端末500は、認証サーバ400から送信されたチケットに含まれるアドレスを用いてアプリケーションサーバ600にチケットを送信すると共にサービスを要求するようになっている。

アプリケーションサーバ600は、ユーザ端末500によって送信されたチケットを記憶し、記憶したチケットに含まれるアドレスとサービスの要求を表すパケットに含まれる送信元アドレスとが一致するか否かを判断し、アドレスが一致すると判断されたときユーザにサービスを提供するようになっている。

なお、本発明の第2の実施の形態に係るアドレスに基づく認証システム2000を構成する手段のうち、本発明の第1の実施の形態に係るアドレスに基づく認証システム1000を構成する構成要素と同一の構成要素には同一の符号を付し、それぞれの説明を省略する。

【0029】

(第2の実施の形態) 認証サーバ

図12は、本発明の第2の実施の形態に係る認証サーバのブロック構成図である。図12に示すように、認証サーバ400は、通信インターフェース101および制御処理手段402を含むように構成される。なお、本発明の第2の実施の形態に係る認証サーバ400を構成する手段のうち、本発明の第1の実施の形態に係る認証サーバ100を構成する手段と同一の手段には同一の符号を付し、それぞれの説明を省略する。

制御処理手段402は、プログラムを処理するCPU(Central Processing Unit)、およびプログラムを記憶するメモリなどを含むように構成される。また、制御処理手段402は、ユーザ認証情報受信手段110、認証手段420、ユーザ識別子割当手段130、アドレス割当手段140、チケット発行手段450、およびチケット送信手段160を有している。なお、これらの手段はプログラムのモジュールでもよい。

認証手段420は、ユーザ認証情報受信手段110によって受信されたユーザ認証情報に基づいてユーザの認証を行うようになっている。例えば、認証手段420は、ユーザ認証情報とユーザデータベース20に格納されている認証データとの整合性を検証(照合)することによってユーザを認証するようになっている。

【0030】

チケット発行手段450は、認証子生成手段151を含むように構成され、アドレス割当手段140によって割当てられたアドレスと、ユーザ識別子割当手段130によって割当られたユーザ識別子と、ユーザ端末500からユーザ認証情報と共に送信された鍵情報と、認証子生成手段151によって生成された認証子とを含むチケットを発行するようになっている。なお、チケットは、他に、チケットを発行したときのタイムスタンプ、チケットの有効期限、ユーザ端末500に割当てられた帯域幅、およびユーザ端末500が収容されるアクセスポイント30に関する情報などによって構成されるようにしてもよい。

なお、チケットの有効期限、およびユーザ端末500に割当られた帯域幅は、アクセスポイント30、認証サーバ400およびアプリケーションサーバ600などを運用する通信事業者やアプリケーションサービス事業者と、ユーザ端末500を使用するユーザとの契約によって予め決められるようにしてもよい。

ここで、図15は、チケットの構成を示す図である。図15に示すように、チケット53は、アドレス、ユーザ識別子、鍵情報、および認証子などによって構成される。

【0031】

(第2の実施の形態) ユーザ端末

図13は、本発明の第2の実施の形態に係るユーザ端末のブロック構成図である。図13に示すように、ユーザ端末500は、通信インターフェース201および制御処理手段502を含むように構成される。なお、本発明の第2の実施の形態に係るユーザ端末500を構成する手段のうち、本発明の第1の実施の形態に係るユーザ端末200を構成する手段と同一の手段には同一の符号を付し、それぞれの説明を省略する。

制御処理手段502は、プログラムを処理するCPU、およびプログラムを記憶するメモリなどを含むように構成される。また、制御処理手段502は、認証要求手段503、およびサービス要求手段530を有している。なお、これらの手段はプログラムのモジュールでもよい。また、認証要求手段503は、ユーザ認証情報入力手段510、ユーザ認証情報送信手段220、およびチケット受信手段231を有している。

ユーザ認証情報入力手段510は、ユーザ認証情報を認証デバイス41から入力させるようになっている。なお、認証デバイス41に格納されたユーザ鍵ペアのうち秘密鍵は、認証デバイス41から持ち出せない。また、認証デバイス41は、ICカード、USB(Universal Serial Bus)キーなどを含むハードウェア認証トークン、または生体認証装置などを含む。

【0032】

なお、認証デバイス41がユーザ端末500に接続されない構成では、ユーザ端末に格納された端末鍵ペアを用いてユーザ認証情報を生成してもよい。

サービス要求手段530は、セッション確立手段532およびパケット処理手段533を含むように構成され、アプリケーションサーバ600が提供するサービスを要求するよ

うになっている。

セッション確立手段532は、ユーザが利用するサービスに応じたアプリケーションサーバ600とのセッションを確立するようになっている。例えば、セッション確立手段532は、チケット受信手段231によって受信されたチケット53を通信インターフェース201を介してアプリケーションサーバ600に送信することにより、セッションを確立するようになっている。

より詳細には、セッション確立手段532は、IKE (Internet Key Exchange)などに準拠して、チケット53に含まれる鍵情報と関連する鍵ペアとアプリケーションサーバ600の公開鍵から計算して得られたセッション秘密鍵をアプリケーションサーバ600と互いに共有するようになっている。

パケット処理手段533は、アプリケーションサーバ600とセッション秘密鍵が共有された後、IPsec (SEcurity architecture for the Internet Protocol)またはTLS (Transport Layer Security)などに準拠して、セッション確立手段532によってアプリケーションサーバ600との間で共有されたセッション秘密鍵を用いてパケットの情報から計算された認証ヘッダをパケットに付加するようになっている。また、パケット処理手段533は、IPsecまたはTLSなどに準拠してパケットを暗号化してもよい。

【0033】

ここで、図16は、認証ヘッダが付加されたパケットの構成の一例を示す図である。認証ヘッダが付加されたパケット54は、送信元アドレスおよび認証ヘッダなどによって構成される。図16に示すように、ユーザ端末500がチケット53をアプリケーションサーバ600に送信するときには、チケット53が認証ヘッダと共にパケット54に含まれていてもよい。

パケット処理手段533は、認証ヘッダが付加されたパケット54を通信インターフェース201を介してアプリケーションサーバ600に送信するようになっている。なお、通信インターフェース201は、チケット受信手段231によって登録されたアドレスを、パケット54に含まれる送信元アドレスに設定し、設定したパケット54を送信するようになっている。

サービス要求手段530は、アプリケーションサーバ600とのセッションが確立された後、サービスの要求を表すパケットをアプリケーションサーバ600に通信インターフェース201に設定したチケット53のアドレスを用いて送信するようになっている。

【0034】

(第2の実施の形態) アプリケーションサーバ

図14は、本発明の第2の実施の形態に係るアプリケーションサーバのブロック構成図である。図14に示すように、アプリケーションサーバ600は、通信インターフェース301および制御処理手段602を含むように構成される。なお、本発明の第2の実施の形態に係るアプリケーションサーバ600を構成する手段のうち、本発明の第1の実施の形態に係るアプリケーションサーバ300を構成する手段と同一の手段には同一の符号を付し、それぞれの説明を省略する。

制御処理手段602は、プログラムを処理するCPU、およびプログラムを記憶するメモリなどを含むように構成される。また、制御処理手段602は、サービス提供手段610、セッション確立手段611、およびチケット記憶手段330を有している。なお、これらの手段はプログラムのモジュールでもよい。

サービス提供手段610は、アドレス判断手段312、およびパケット認証手段612を含むように構成され、ユーザ端末500から要求されるサービスを提供するようになっている。

【0035】

セッション確立手段611はチケット検証手段620を含むように構成され、ユーザ端末500とのセッションを確立するようになっている。なお、セッションを確立する手順の中で、セッション確立手段611は、IKEなどに準拠してセッション秘密鍵をユーザ端末500と互いに共有するようになっている。

パケット認証手段612は、ユーザ端末500とセッション秘密鍵が共有された後、受信したパケットに付加された認証ヘッダをセッション秘密鍵を用いて認証するようになっている。また、パケット認証手段612は、チケット53を含むパケット54に付加された認証ヘッダの認証結果が正常であったとき、チケット53をチケット検証手段620に出力するようになっている。

チケット検証手段620は、パケット認証手段612によって出力されたチケット53の正当性を検証するようになっている。さらに、チケット検証手段620において、チケット53に含まれる鍵情報とセッション秘密鍵の共有に用いたユーザ側の公開鍵を照合し、チケット53に含まれるアドレスとパケット54に含まれる送信元アドレスとを照合した結果、それらが一致した場合、チケット記憶手段330は、チケット53を記憶するようになっている。

サービス提供手段610は、ユーザ端末500とのセッションが確立された後、IPsecまたはTLS等に準拠してインテグリティチェックもしくは復号化されたパケットに含まれる送信元アドレスとチケット53に含まれるアドレスとが一致したとアドレス判断手段312によって判断されたとき、ユーザ端末500から要求されるサービスを提供するようになっている。

【0036】

(第2の実施の形態) アドレスに基づく認証システムの処理

以下、本発明の第2の実施の形態に係るアドレスに基づく認証システムの処理について、図面を参照して説明する。図17は、本発明の第2の実施の形態に係るアドレスに基づく認証システムの処理を示すシーケンス図である。

まず、ユーザの認証を要求するとき、ユーザ認証情報が、ユーザ端末500によってアクセスポイント30を介して送信される。ユーザ端末500から送信されたユーザ認証情報に基づいて、ユーザの認証が認証サーバ400によって行われる。ユーザの認証が成功したとき、割当てたアドレス、ユーザ識別子、および鍵情報を含むチケット53が、認証サーバ400によって発行され、ユーザ端末500に送信される。

ユーザ端末500とアプリケーションサーバ600とのセッションの確立を要求するとき、IKEなどの鍵交換手順に準拠して互いの鍵ペアから計算して得られたセッション秘密鍵が、ユーザ端末500とアプリケーションサーバ600との間で共有される。すなわち、ユーザ端末500は自己の鍵ペアとアプリケーションサーバ600の公開鍵を用い、また、アプリケーションサーバ600は自己の鍵ペアとユーザ端末500の公開鍵を用いてセッション秘密鍵を計算する。セッション秘密鍵が互いに共有された後、セッション秘密鍵を用いて生成された認証ヘッダが付加されたパケットは、ユーザ端末500からアプリケーションサーバ600に送信される。パケットに付加された認証ヘッダは、アプリケーションサーバ600によって認証される。

【0037】

ここで、ユーザ端末500が認証ヘッダを付加したパケットのうち、チケット53を含むパケット54が、ユーザ端末500によって送信されたとき、アプリケーションサーバ600によって、受信されたチケット53の正当性が検証され、チケット53に含まれる鍵情報がセッション秘密鍵の共有に用いられたユーザ側の公開鍵(ユーザ公開鍵もしくは端末公開鍵)と対応するか否かが検証される。さらにチケット53を含むパケット54の送信元アドレスと、チケット53に含まれるアドレスがアプリケーションサーバ600により照合される。チケット53が正当であり、かつ鍵情報がユーザ側の公開鍵と対応し、かつパケット54の送信元アドレスとチケット53に含まれるアドレスが一致するとき、チケット53が記憶され、セッションが確立される。

次に、ユーザ端末500とアプリケーションサーバ600とのセッションが確立された後、アプリケーションサーバ600に対してサービスを要求するとき、サービスの要求を表すパケットは、送信元アドレスを保護するため暗号化処理または認証ヘッダ付加処理のうち少なくとも1つが施され、ユーザ端末500によってアプリケーションサーバ600に送信される。記憶したチケット53に含まれるアドレスと、暗号化処理または認証ヘッ

タ付加処理に対応した復号化処理して得られたサービス要求を表すパケットに含まれるアドレスとが一致するか否かがアプリケーションサーバ600によって判断され、アドレスが一致すると判断されたときサービスがユーザに提供される。

【0038】

(第2の実施の形態) 認証サーバの処理

図18は、本発明の第2の実施の形態に係る認証サーバの処理の流れを示すフローチャートである。なお、本発明の第2の実施の形態に係る認証サーバの処理のうち、本発明の第1の実施の形態に係る認証サーバの処理と同一のものについては、同一の符号を付しそれぞれの説明を省略する。

ユーザ認証情報に基づいて認証手段420によってユーザの認証が行われ、ユーザの認証が成功したとき、処理はS103へ進み、ユーザの認証が失敗したとき、処理は終了する(S401)。ユーザの認証が成功したとき、ユーザ端末から鍵情報を受信し、アドレス、ユーザ識別子、および鍵情報を含むチケット53は、チケット発行手段450によって発行される(S402)。

【0039】

(第2の実施の形態) ユーザ端末の処理

図19は、本発明の第2の実施の形態に係るユーザ端末の処理の流れを示すフローチャートである。なお、本発明の第2の実施の形態に係るユーザ端末の処理のうち、本発明の第1の実施の形態に係るユーザ端末の処理と同一のものについては、同一の符号を付しそれぞれの説明を省略する。

ユーザ認証情報は、ユーザ認証情報入力手段510によって入力され(S501)、ユーザ認証情報送信手段220によって通信インターフェース201を介して認証サーバ400に送信される(S202)。認証サーバ400から送信されたチケット53は、チケット受信手段231によって受信される(S203)。

その後、アプリケーションサーバ600とのセッションの確立は、セッション確立手段532によって開始され、セッション秘密鍵が、ユーザ端末500とアプリケーションサーバ600との間で共有される。ここで、チケット53を含むパケット54は、パケット処理手段533によって認証ヘッダ付加処理および暗号化処理が施され、アプリケーションサーバ600に送信される(S502)。

次に、アプリケーションサーバ600とのセッションが確立された後、サービスの要求を表すパケットは、サービス要求手段530によってセッションを通してアプリケーションサーバ600に送信されることによって、サービスがアプリケーションサーバ600に要求される(S205)。

【0040】

(第2の実施の形態) アプリケーションサーバの処理

図20は、本発明の第2の実施の形態に係るアプリケーションサーバの処理の流れを示すフローチャートである。なお、本発明の第2の実施の形態に係るアプリケーションサーバの処理のうち、本発明の第1の実施の形態に係るアプリケーションサーバの処理と同一のものについては、同一の符号を付しそれぞれの説明を省略する。

まず、ユーザ端末500とのセッションの確立は、セッション確立手段611によって開始され、IKEなどの鍵交換手順に準拠して互いの鍵ペアから計算して得られたセッション秘密鍵が、ユーザ端末500とアプリケーションサーバ600との間で共有される(S601)。ここで、ユーザ端末500によって送信されたチケット53を含むパケット54が、アプリケーションサーバ600によって受信される。

受信されたパケット54に付加された認証ヘッダは、パケット認証手段612によって、セッション秘密鍵を用いて認証され、認証ヘッダが正しいと認証された場合、処理はS302に進み、パケット54が改竄されているなど正しくないと検証された場合、処理は終了する(S602)。

【0041】

チケット53の正当性が検証され、チケットに含まれる鍵情報をと、セッション秘密鍵の

共有に用いたユーザ側の公開鍵との整合性が検証され、パケット54に含まれる送信元アドレスとチケットに含まれるアドレスが一致している場合には、チケット53は正しいものとして、チケット記憶手段330によって記憶される(S302)。

ユーザ端末500から送信されたサービスを要求するパケットに含まれる送信元アドレスは、記憶したチケット53に含まれるアドレスと一致するか否かが判断され、アドレスが一致すると判断されたとき、サービス提供手段610によってユーザ端末500を介してユーザにサービスが提供される(S304)。

なお、ユーザ端末500がチケット53を含むパケット54をアプリケーションサーバ600に送信するタイミングにおいては、IKEなどの鍵交換手順の中で送信されてもよい。この場合には、セッション秘密鍵が共有される前であるため、チケットを含むパケット54には、認証ヘッダが付加されないが、チケット53に基づいて鍵交換手順中の所定のステップを開始するか否かを判断することができる。

以上説明したように、本発明の第2の実施の形態に係るアドレスに基づく認証システムは、ユーザ端末500が、セッション秘密鍵を用いてパケットの情報から計算された認証ヘッダをパケットに付加して送信し、アプリケーションサーバ600が、ユーザ端末500から送信されたパケットに付加された認証ヘッダを認証するため、ユーザ端末500とアプリケーションサーバ600との間で送受されるパケット54のインティグリティを保証することができる。

また、チケット53が正しいことを検証したときチケット53を記憶させるため、認証サーバ400によって発行されたチケット53の正当性を保証することができる。また、認証サーバ400が、アドレス、ユーザ識別子、および鍵情報を含むチケット53を発行し、ユーザ端末500が、発行されたチケット53をアプリケーションサーバ600に送信し、アプリケーションサーバ600が、送信されたチケット53を記憶し、記憶したチケット53に含まれるアドレスに基づいてユーザ端末500から送信されたパケットを、認証されたユーザのパケットとみなすことにより、アドレスに基づく認証が可能となる。

【図面の簡単な説明】

【0042】

【図1】本発明の第1の実施の形態に係るアドレスに基づく認証システムのシステム構成図。

【図2】本発明の第1の実施の形態に係る認証サーバのブロック構成図。

【図3】本発明の第1の実施の形態に係るユーザ端末のブロック構成図。

【図4】本発明の第1の実施の形態に係るアプリケーションサーバのブロック構成図

。

【図5】本発明の第1の実施のチケットの構成を示す図。

【図6】本発明の第1の実施の暗号化されたパケットの構成及びアプリケーションサーバの処理を示す図。

【図7】本発明の第1の実施の形態に係るアドレスに基づく認証システムの処理を示すシーケンス図。

【図8】本発明の第1の実施の形態に係る認証サーバの処理の流れを示すフローチャート。

【図9】本発明の第1の実施の形態に係るユーザ端末の処理の流れを示すフローチャート。

【図10】本発明の第1の実施の形態に係るアプリケーションサーバの処理の流れを示すフローチャート。

【図11】本発明の第2の実施の形態に係るアドレスに基づく認証システムのシステム構成図。

【図12】本発明の第2の実施の形態に係る認証サーバのブロック構成図。

【図13】本発明の第2の実施の形態に係るユーザ端末のブロック構成図。

【図14】本発明の第2の実施の形態に係るアプリケーションサーバのブロック構成図。

【図15】本発明の第2の実施のチケットの構成を示す図。

【図16】本発明の第2の実施の認証ヘッダが付加されたパケットの構成及びアプリケーションサーバの処理を示す図。

【図17】本発明の第2の実施の形態に係るアドレスに基づく認証システムの処理を示すシーケンス図。

【図18】本発明の第2の実施の形態に係る認証サーバの処理の流れを示すフローチャート。

【図19】本発明の第2の実施の形態に係るユーザ端末の処理の流れを示すフローチャート。

【図20】本発明の第2の実施の形態に係るアプリケーションサーバの処理の流れを示すフローチャート。

【符号の説明】

【0043】

10 ネットワーク

20 ユーザデータベース

30 アクセスポイント

40 入力機器

41 認証デバイス

51、53 チケット

52、54 パケット

100、400 認証サーバ

101、201、301 通信インターフェース

102、202、302、402、502、602 制御処理手段

110 ユーザ認証情報受信手段

120、420 認証手段

130 ユーザ識別子割当手段

140 アドレス割当手段

150、450 チケット発行手段

151 認証子生成手段

160 チケット送信手段

200、500 ユーザ端末

203、503 認証要求手段

210 ユーザ認証情報生成手段

220 ユーザ認証情報送信手段

230、530 サービス要求手段

231 チケット受信手段

232、311、532、611 セッション確立手段

300、600 アプリケーションサーバ

310、610 サービス提供手段

312 アドレス判断手段

320、620 チケット検証手段

330 チケット記憶手段

510 ユーザ認証情報入力手段

533 パケット処理手段

612 パケット認証手段

1000、2000 アドレスに基づく認証システム

【書類名】 図面
【図1】

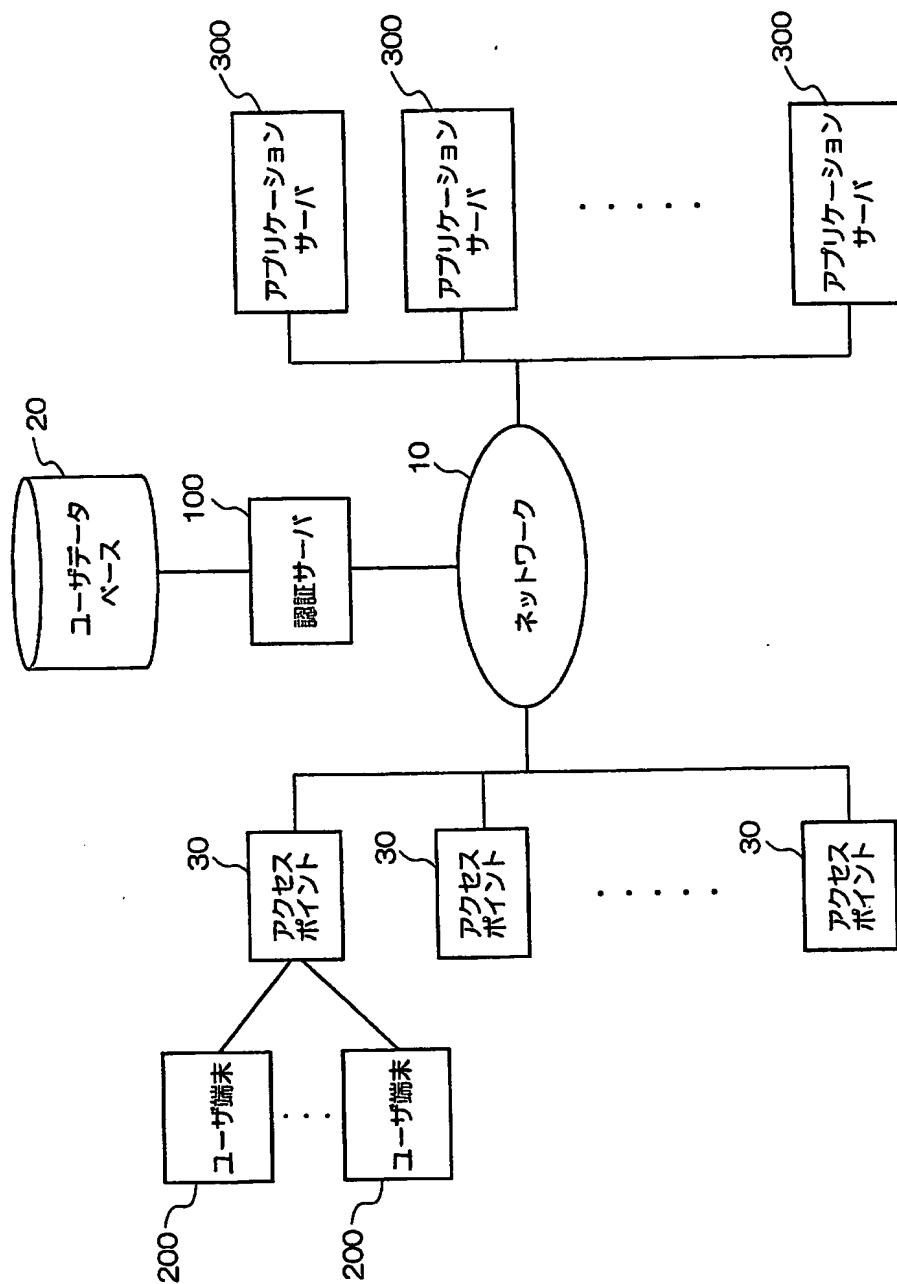


図1
(第4の実験の形態) ユドリフに基因組と認証システィ/1000の構成

【図2】

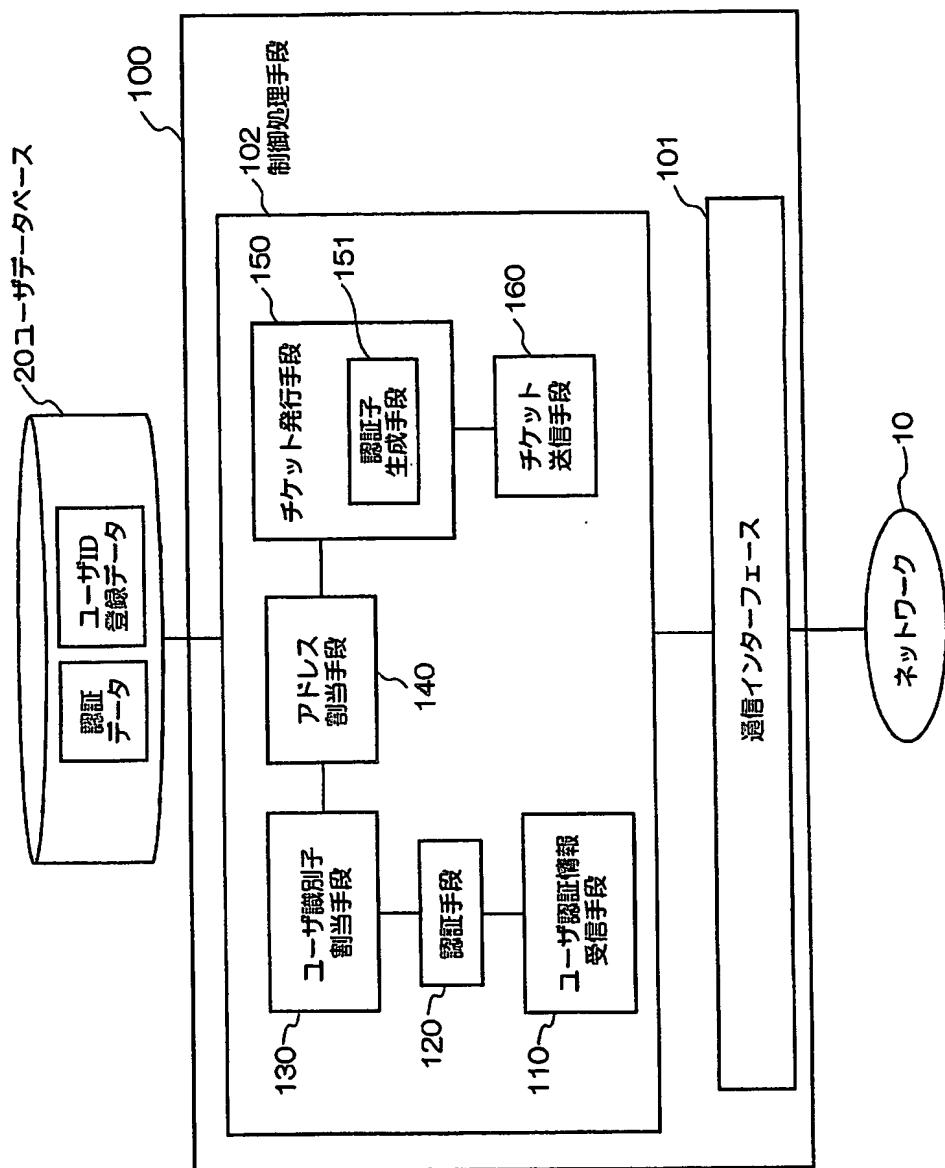


図2

(第1の実施の形態) 認証サーバ100の構成

【図3】

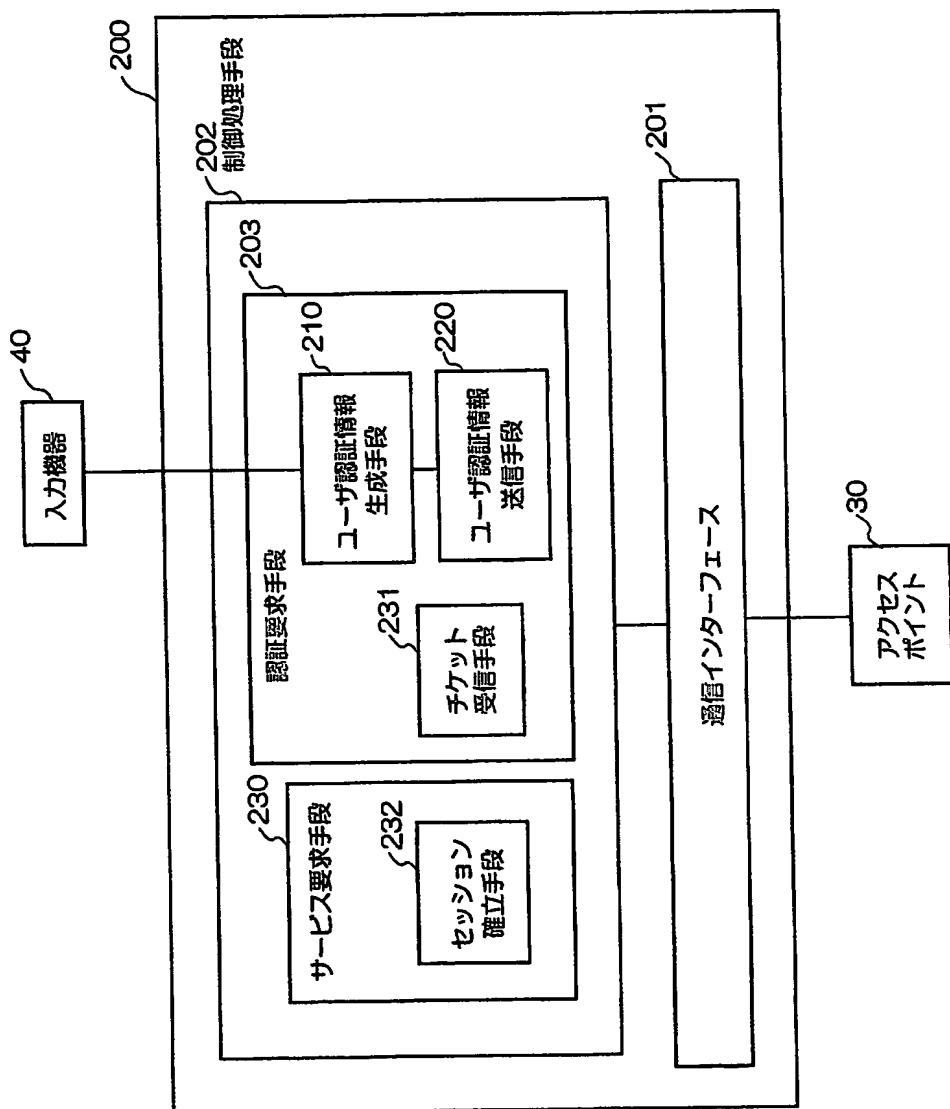
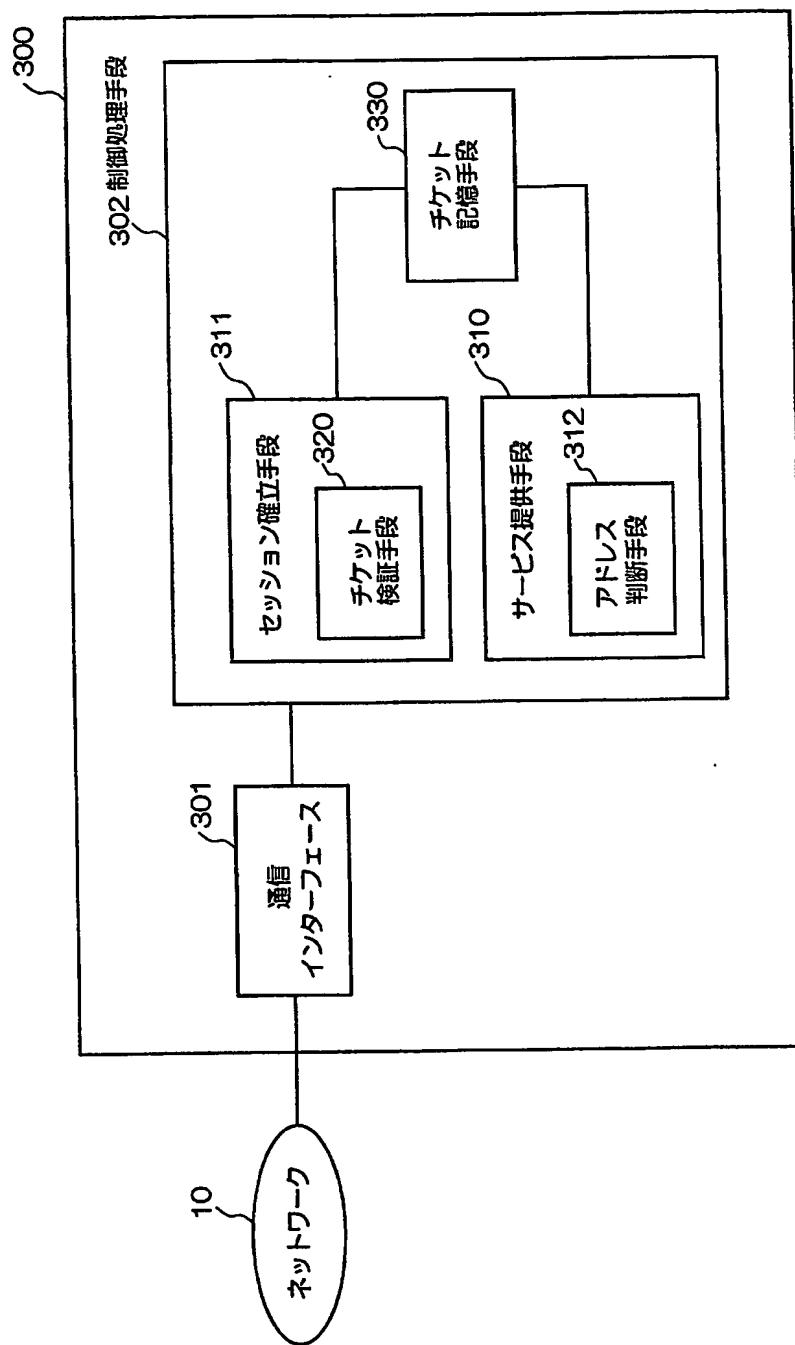


図3

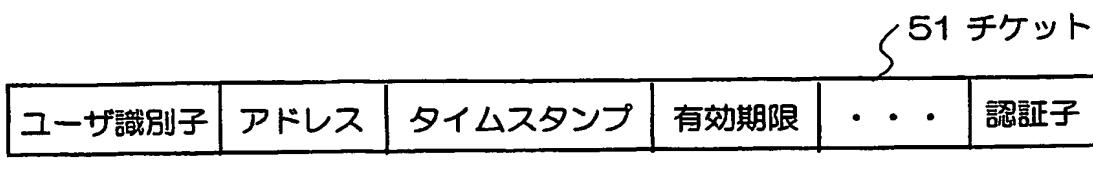
(第1の実施の形態) ユーザ端末200 の構成

【図4】



(第1の実施の形態) アプリケーションサーバ300 の構成 図4

【図5】



ユーザ識別子：ユーザと対応する識別子
 アドレス：ユーザ識別子と対応させて割当
 タイムスタンプ：チケット発行作成日時
 有効期限：チケット有効期限
 認証子：アプリケーションサーバと共有する秘密鍵を用いて生成

(第1の実施の形態) チケット51の構成

図5

【図6】

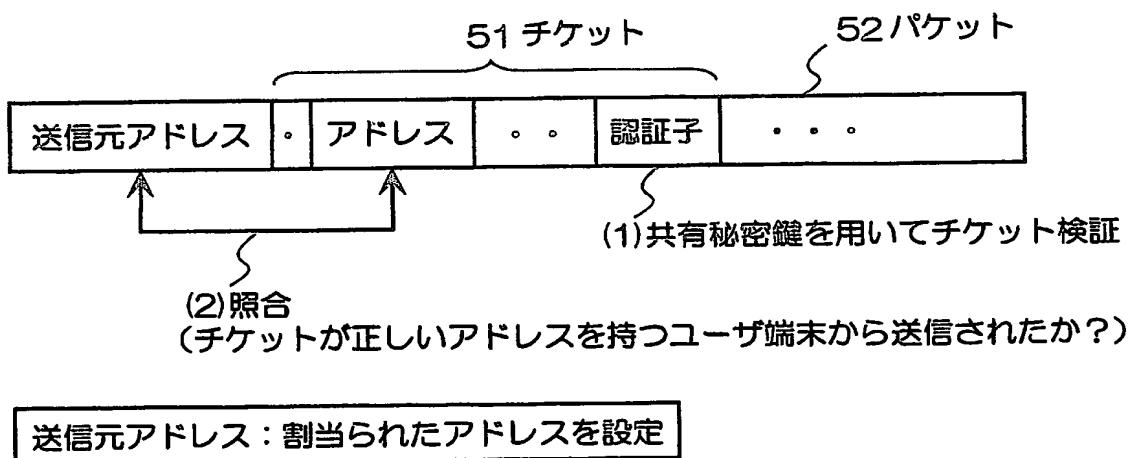
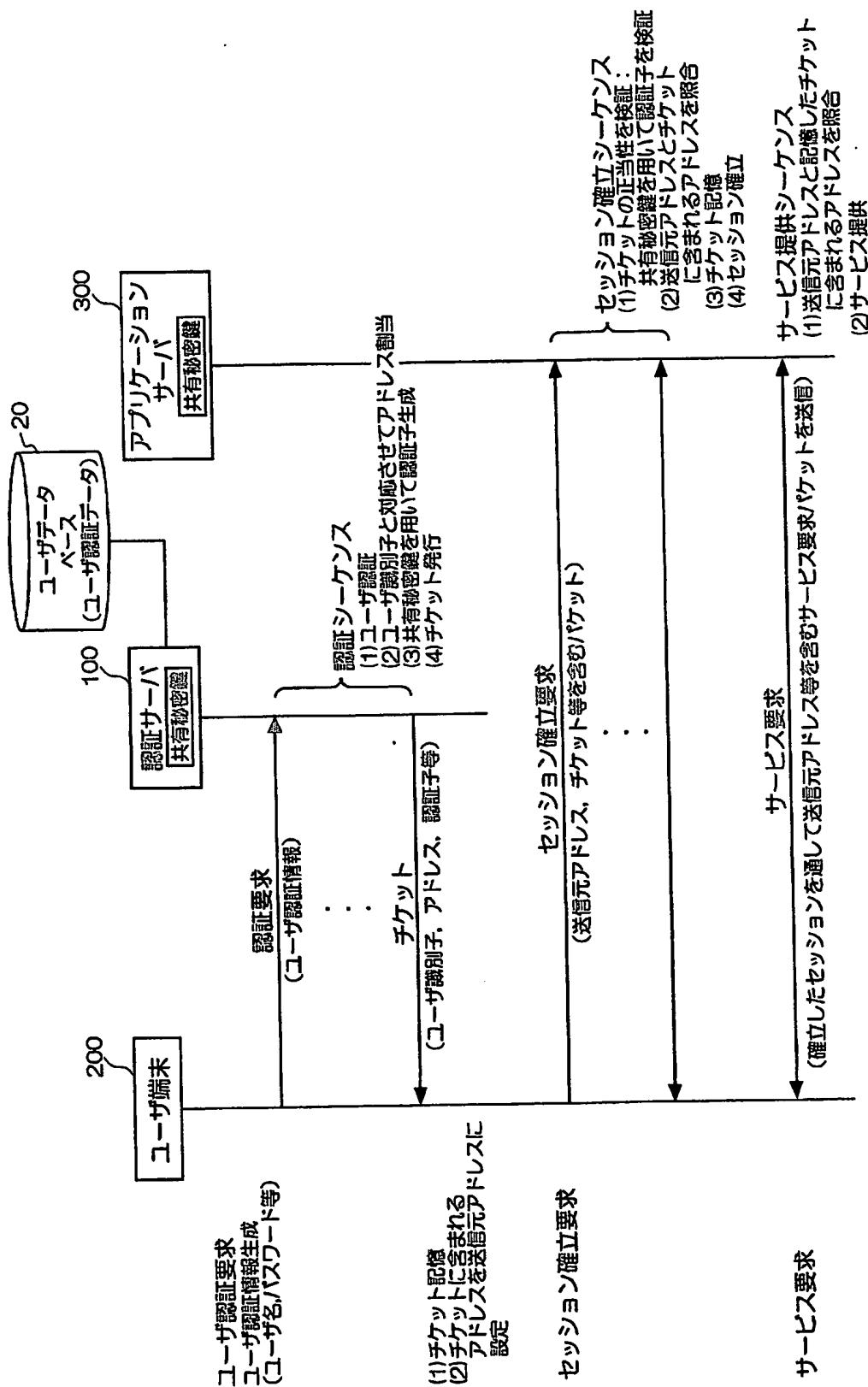
(第1の実施の形態) チケット送信時のパケット52の構成
及びアプリケーションサーバの処理

図6

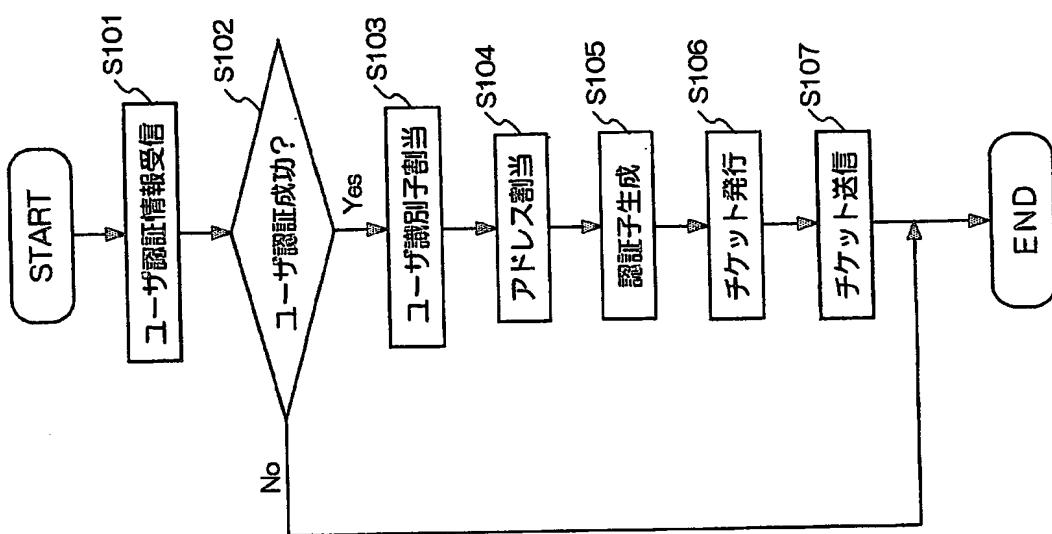
【図 7】



(第1の実施の形態) アドレスに基づく認証システムの処理を示すシーケンス

図7

【図8】



(第1の実施の形態) 認証サーバ100の処理の流れを示すフローチャート 図8

【図9】

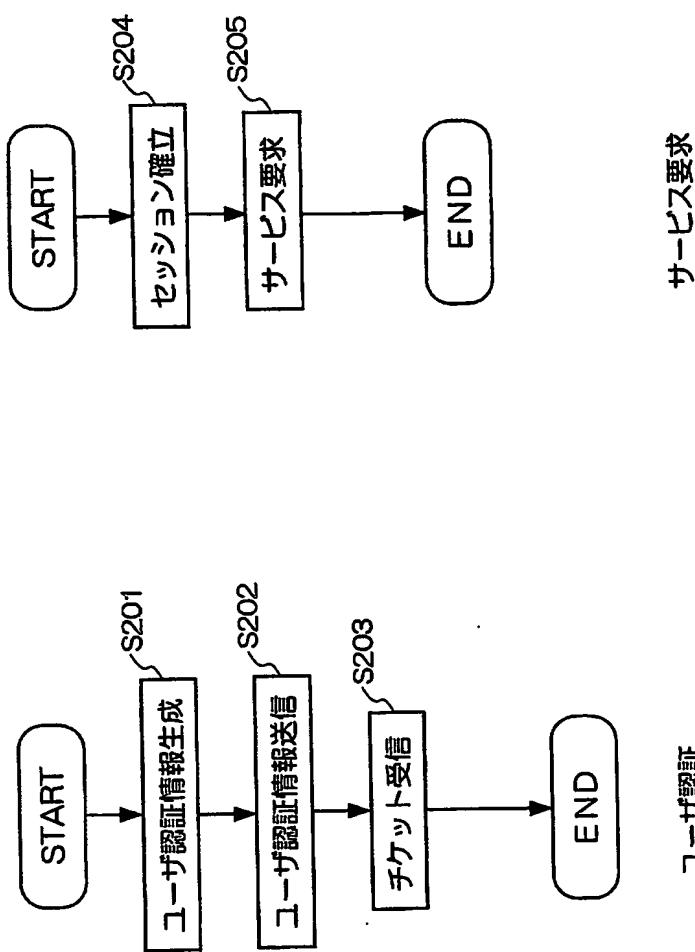


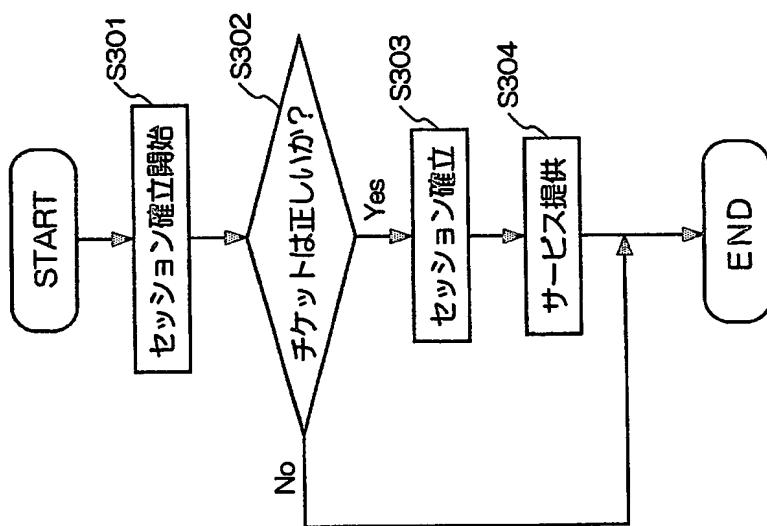
図9

(第1の実施の形態) ユーザ端末200の処理の流れを示すフローチャート

サービス要求

ユーザ認証

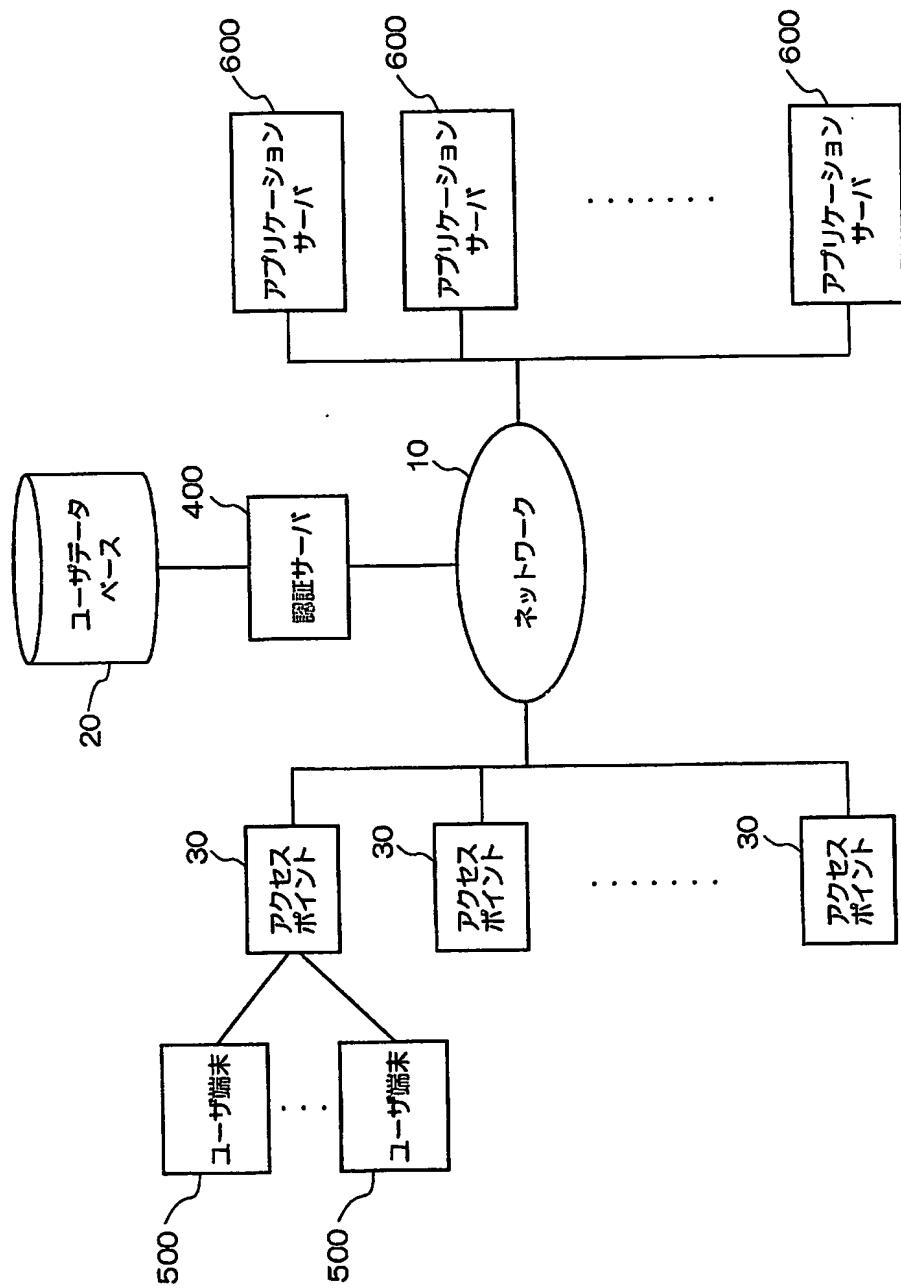
【図10】



(第1の実施の形態) アプリケーションサーバ300の処理の流れを示すフローチャート

図10

【図11】



四

(第2の実施の形態) アドレスに基づく認証システム2000の構成

【図12】

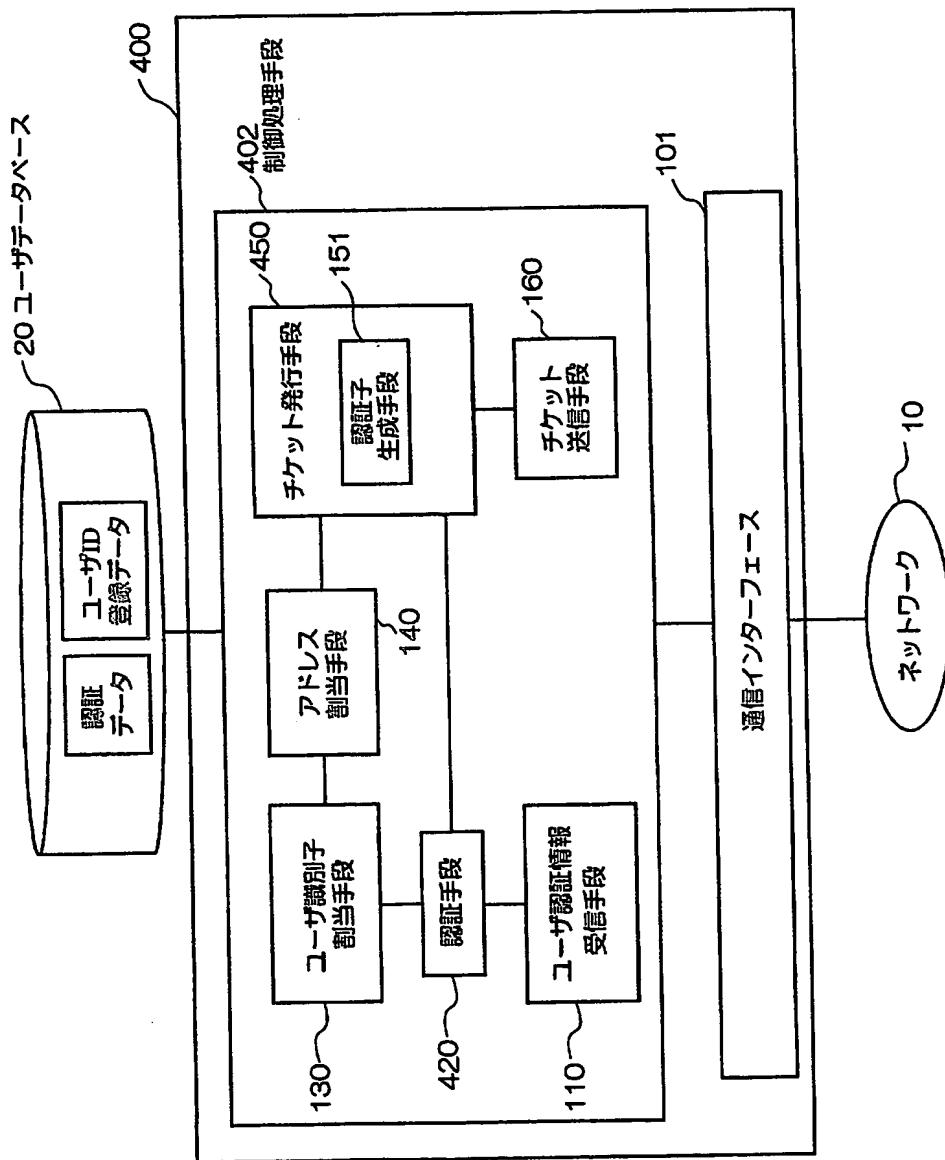


図12

(第2の実施の形態) 認証サーバー/400 の構成

【図13】

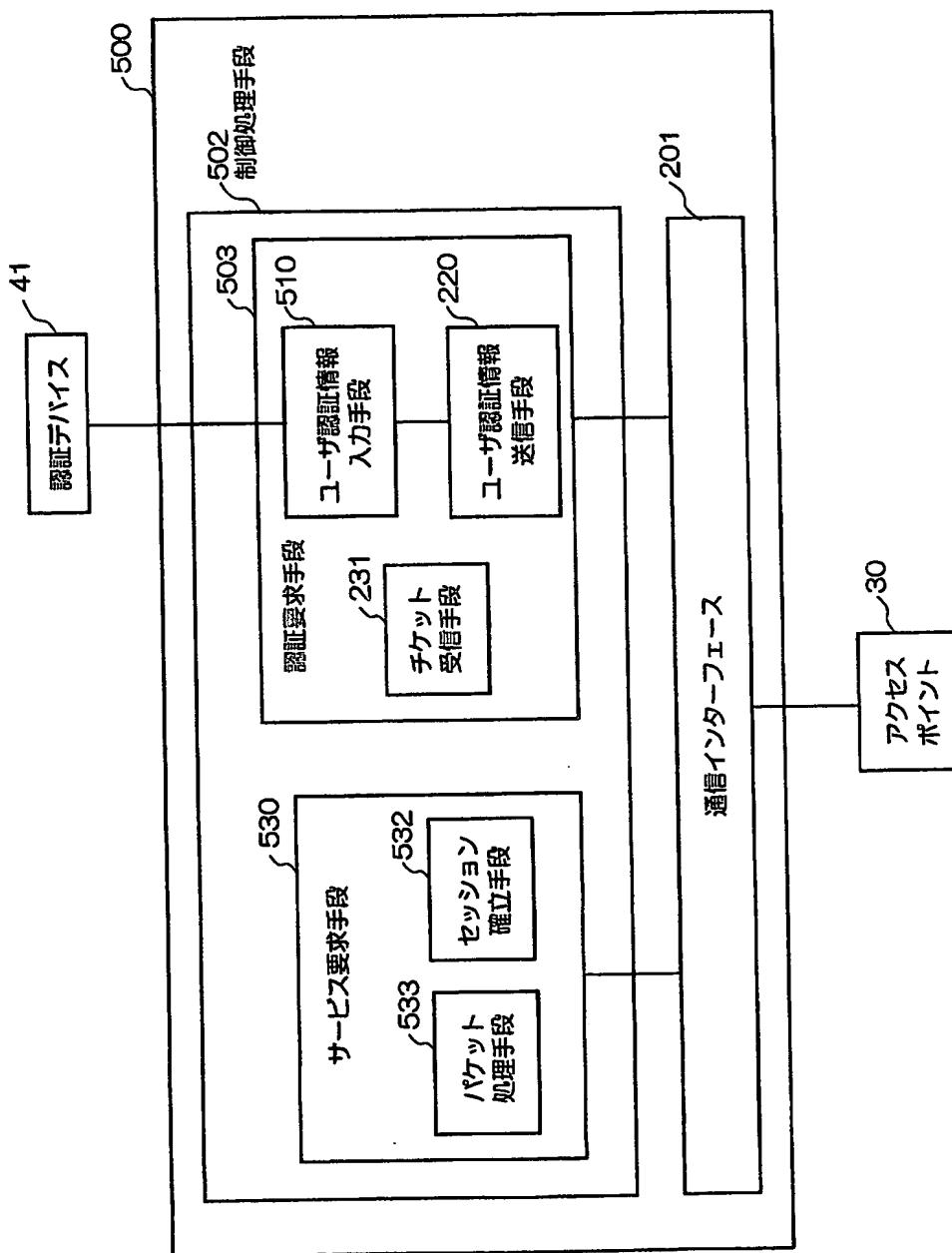


図13

(第2の実施形態) ユーザ端末500の構成

【図14】

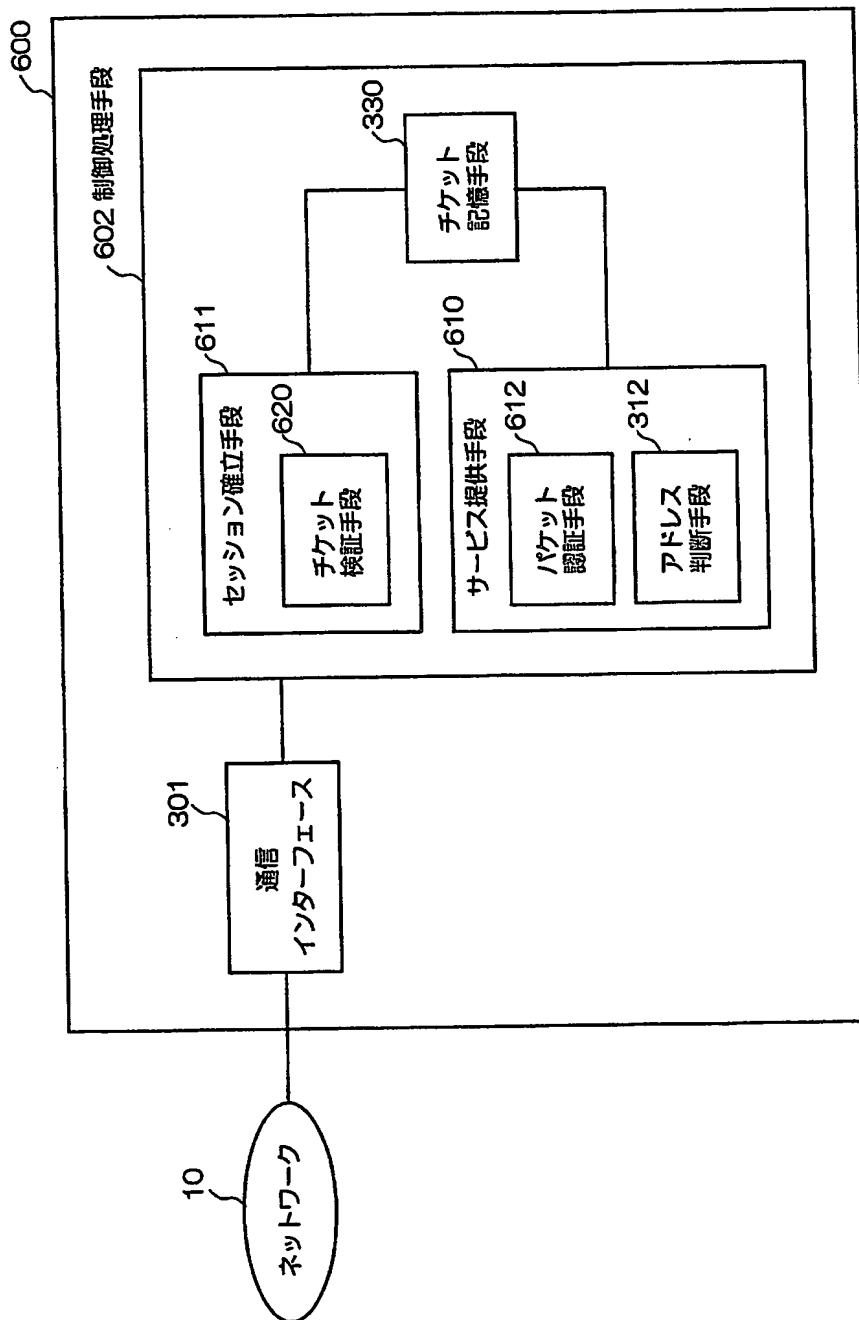
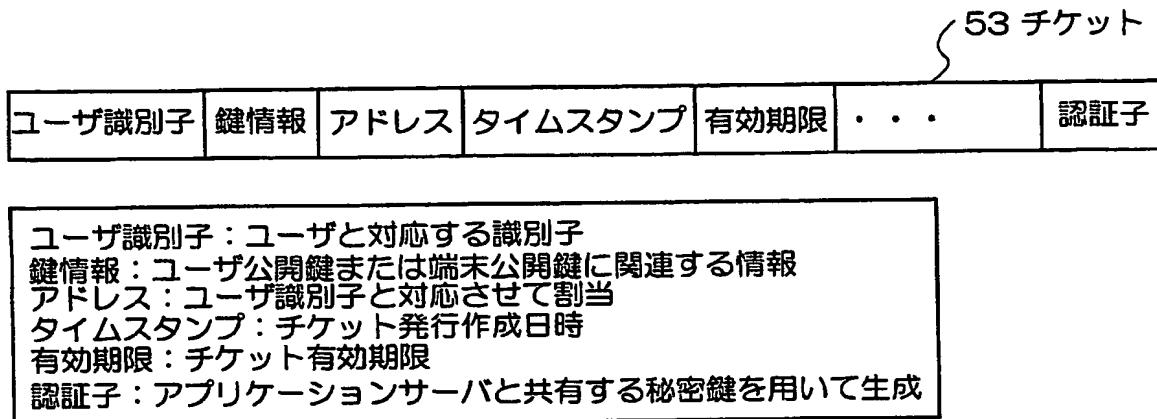


図14

(第2の実施の形態) アプリケーションサーバー/6000の構成

【図 15】



(第2の実施の形態) チケット53の構成

図15

【図 16】

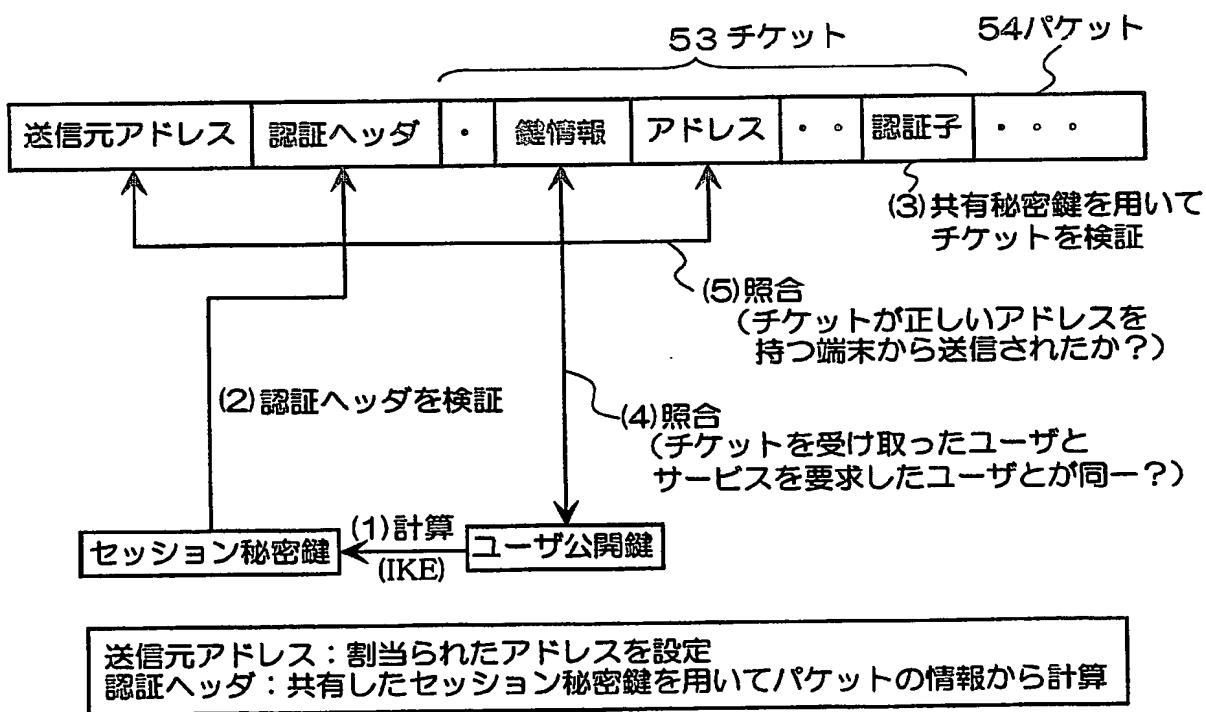
(第2の実施の形態) チケット送信時のパケット54の構成
及びアプリケーションサーバの処理

図16

【図 17】

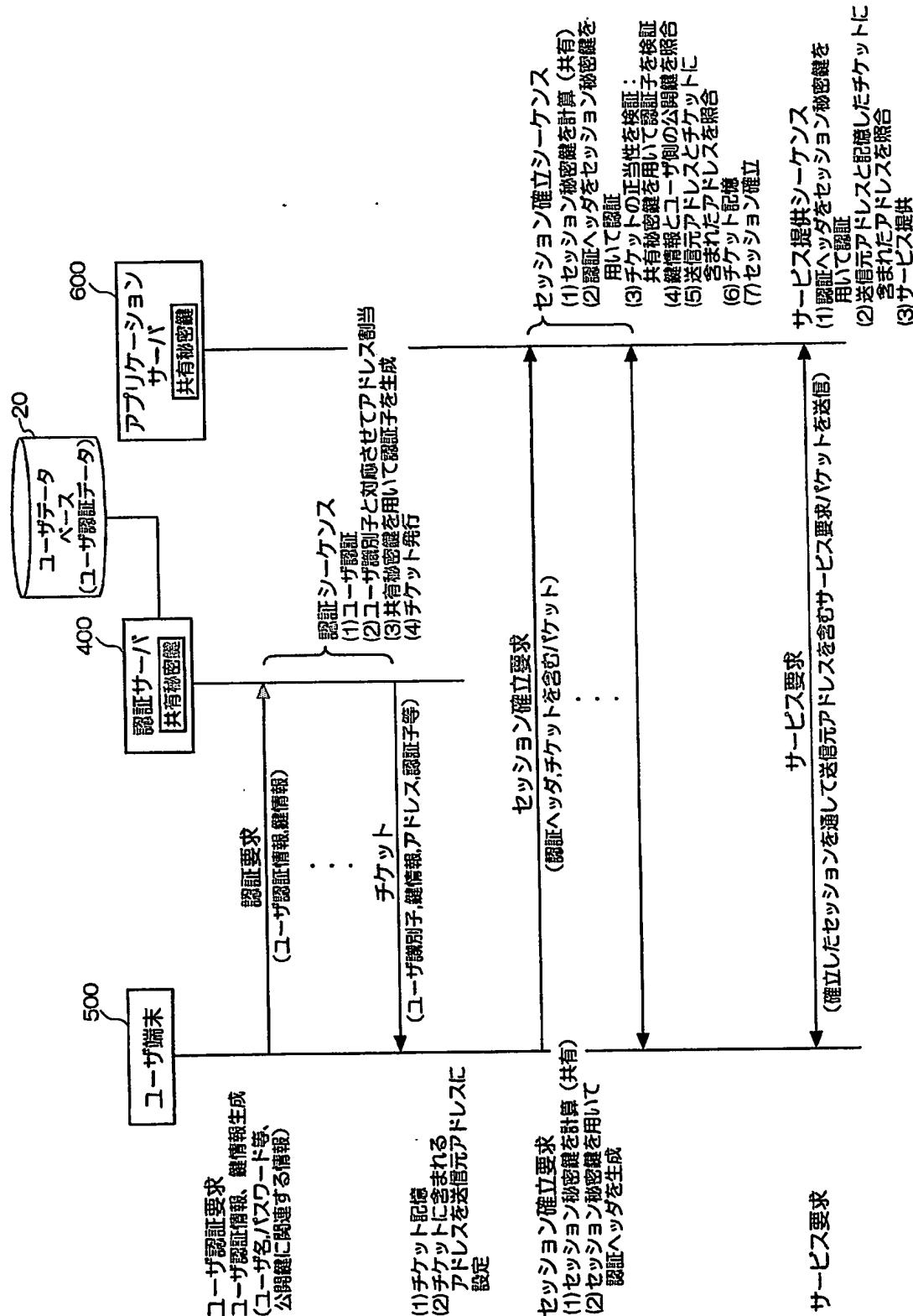
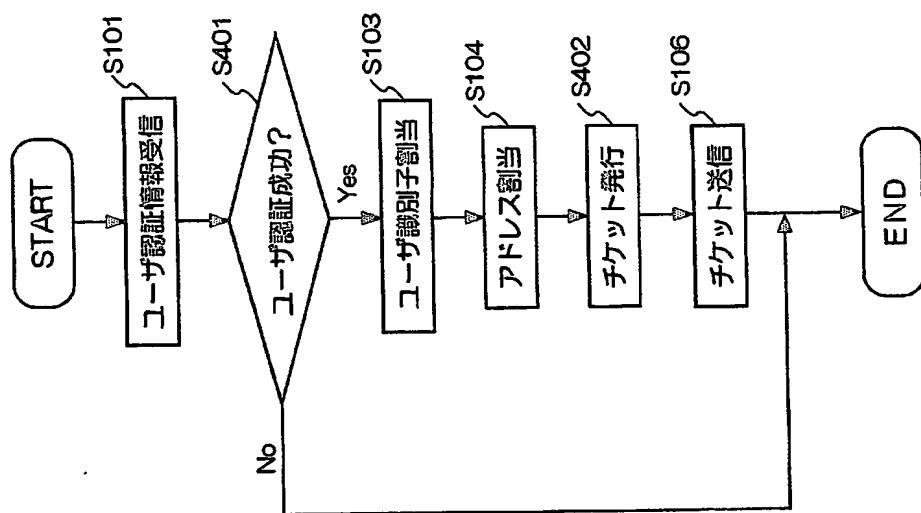


図 17

【図18】



(第2の実施の形態) 認証サーバ400の処理の流れを示すフローチャート 図18

【図19】

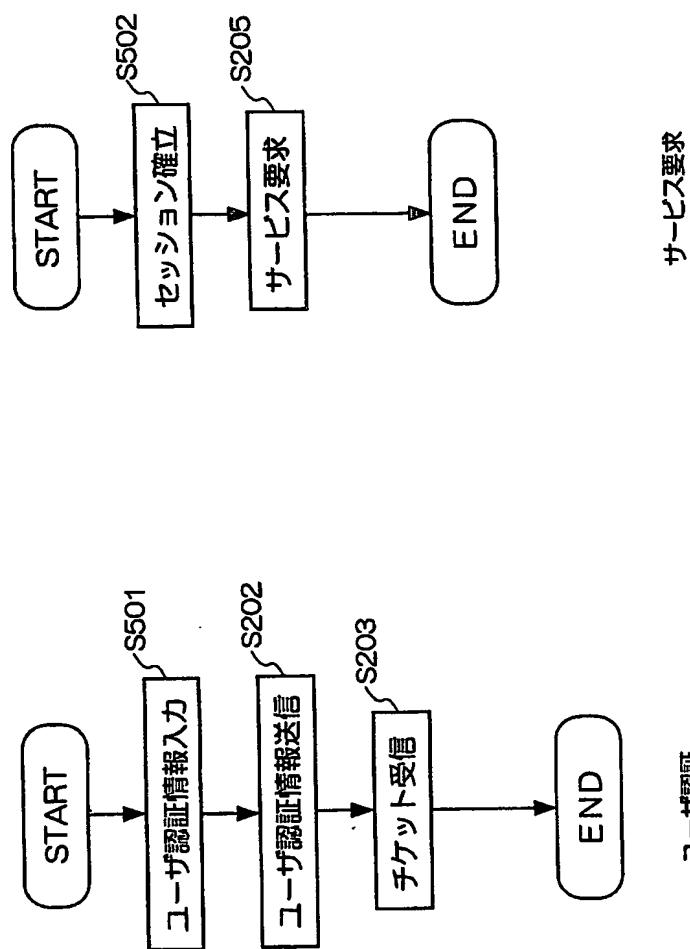
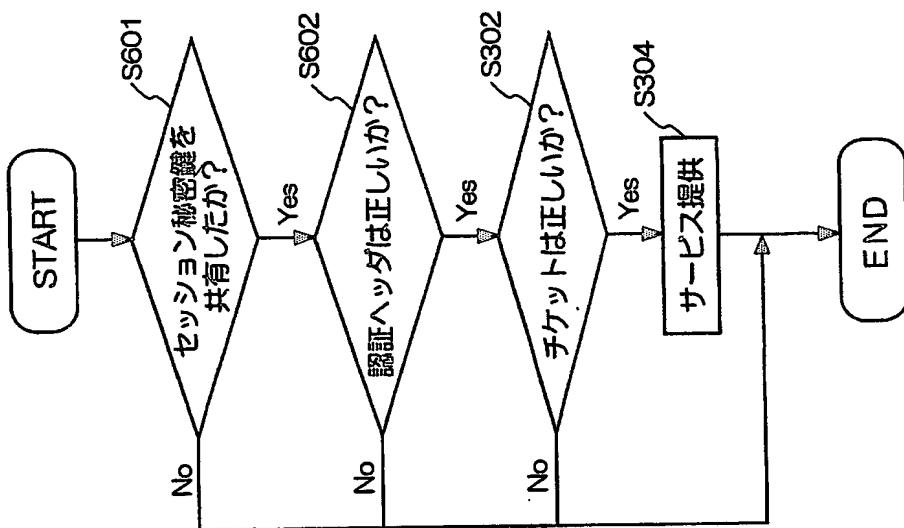


図19

(第2の実施の形態) ユーザ端末500の処理の流れを示すフローチャート

【図20】



(第2の実施の形態) アプリケーションサーバ600の処理の流れを示すフローチャート

図20

【書類名】要約書

【要約】

【課題】ユーザに割当てたアドレスの正当性を保証することができるアドレスに基づく認証システムを提供する。

【解決手段】認証サーバ100はユーザ端末200から送信されたユーザ認証情報に基づいてユーザの認証を行い、認証が成功した時、ユーザ端末に割当てたアドレスを含むチケットを発行してユーザ端末200に送信する。ユーザ端末はチケットに含まれるアドレスを送信元アドレスに設定し、アプリケーションサーバ300にチケットを送信してセッションの確立を要求する。アプリケーションサーバはチケットの正当性を検証した後、チケットを記憶し、ユーザ端末とのセッションを確立する。ユーザ端末は、このセッションを用いて送信元アドレスを含むサービスを要求するパケットをアプリケーションサーバに送信する。アプリケーションサーバは、送信元アドレスと記憶したチケットに含まれるアドレスとが一致した時、ユーザにサービスを提供する。

【選択図】 図1

特願 2003-273445

出願人履歴情報

識別番号 [000004226]

1. 変更年月日 1999年 7月15日

[変更理由] 住所変更

住 所 東京都千代田区大手町二丁目3番1号

氏 名 日本電信電話株式会社